华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*）享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：*关联证书*后，请提交您的“华为账号”和注册账号的“email”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训/面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见*LVC排期*
- **4、学习工具 eNSP**
  - eNSP (Enterprise Network Simulation Platform), 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外, 华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html）

HUAWEI构建安全网络架构工程师培训上机指导书

（学员用书）

ISSUE 1.00



Contents

1 手册说明

本手册用于指导学员学习华为安全产品的配置和部署技术，学员可以通过教材的实验说明，掌握本手册中的实验内容。

1.1 适用范围

适用于华为系统安全高级工程师培训安全课程中涉及的实验内容。
适用安全产品系列包括：

USG2100

USG2200

USG5100

USG5500

USG9500

1.2 适用防火墙产品描述

1.2.1 USG2000 产品描述

1.2.1.1 USG2100 产品外观

USG2100 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 420mm×255mm×43.6mm（宽×深×高），可以安装在 19 英寸标准机柜中。

1.2.1.2 USG2100 部件分布

前面板

如下图所示，USG2100 前面板上有 3G 数据卡接口（仅 USG2130 支持）、USB 接口、Flash 卡接口、指示灯和系统复位键。
USG2120 的前面板上无 3G 数据卡接口，其他部分和 USG2130 的前面板完全一样。

Figure 1-1 USG2100 前面板图



1. 3G 数据卡接口	2. USB 接口	3. Flash 卡接口
4. 指示灯	5. 系统复位键	

后面板

如下图所示，USG2100 后面板包括交流电源模块、MIC(Mini Interface Card)插槽、Console 接口和以太网口等。其中 WAN 口为路由口，可直接配置 IP 地址，并直接划到具体的区域里。LAN 口为交换口，不能在接口上配置 IP 地址，需要先创建 VLAN，然后在 VLAN 上配置 VLAN interface，再把该 VLAN 划到具体的区域里。

Figure 1-2 USG2100 后面板



1. 接地端子	2. 安全锁孔	3. 防静电手腕插孔
4. WAN 接口	5. LAN 接口	6. Console 口
7. MIC 插槽	8. 交流电源开关	9. 交流电源接口

1.2.1.3 USG2200 产品外观

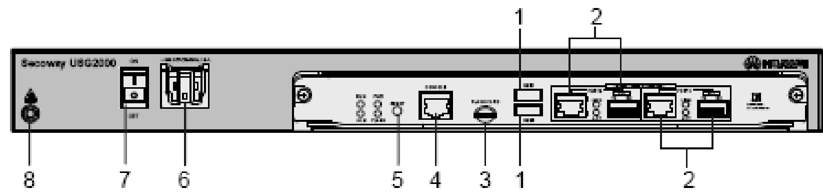
USG2200 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×43.6mm（宽×深×高），可以安装在 19 英寸标准机柜中。

1.2.1.4 USG2200 部件分布

前面板

USG2200 的电源和风扇采用内置式，因此从外观上看不到电源和风扇。USG2200 包括 USG2210、USG2220、USG2230、USG2250 四种型号。这四种型号都支持交流机型，前面板如下图所示。前面板左侧分别为防静电插孔，电源开关和交流电源插孔；右侧包括的固定接口包括：1 个 Console 接口、2 个 GE Combo 接口、2 个 USB2.0 接口、1 个闪存接口。

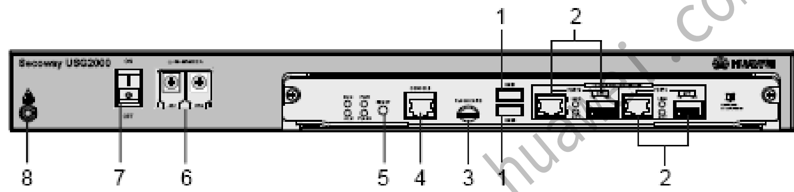
Figure 1-3 USG2200 产品交流机型前面板



1. USB2.0 接口	2. GE Combo 接口	3. 闪存接口
4. Console 接口	5. 一键恢复	6. 交流电源插孔
7. 交流电源开关	8. 防静电手腕插孔	

其中 USG2250 还支持直流机型，其前面板如下图所示。

Figure 1-4 USG2250 产品直流机型前面板

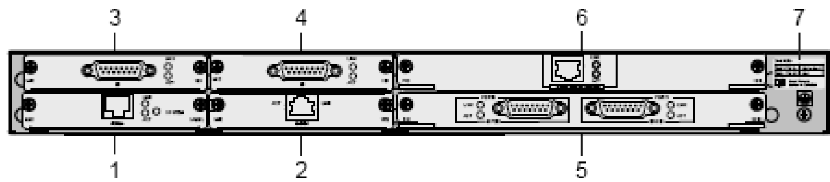


1. USB2.0 接口	2. GE Combo 接口	3. 闪存接口
4. Console 接口	5. 一键恢复	6. 直流电源插孔
7. 直流电源开关	8. 防静电手腕插孔	

后面板

USG2210、USG2220、USG2230、USG2250 后面板布局相同，如下图所示，左侧和中间是 4 个 MIC 插槽，右侧为 2 个 FIC 插槽。如果选用的插卡为交换插卡，该交换插卡上的接口配置方式与 USG2100 上的 LAN 口配置方法一致。如果选用插卡的接口为路由口，则配置方式与 USG3000/USG5000 或者 USG2100 上的 WAN 口配置方式一致。

Figure 1-5 USG 产品后面板



1. MIC1 插槽	2. MIC2 插槽	3. MIC3 插槽
4. MIC4 插槽	5. FIC5 插槽	6. FIC6 插槽
7. 槽位标识		

1.2.1.5 插槽的排列顺序及接口编号方法

下面介绍 USG2200 插槽的排列顺序及接口编号方法。

插槽排列顺序

USG2200 主板编号为 0，其 6 个扩展插槽的槽位编号（1 ～ 6）采用先从左到右，再从下到上，先 MIC 槽位后 FIC 槽位的编号原则。

接口编号方法

设备接口采用的编号原则如下：

1. 接口编号为 interface-type X/0/Y，interface-type 为接口类型（如 Ethernet 等），X 表示槽位号，0 为板卡号，目前支持的接口卡没有子卡，所以此位均为 0。Y 表示接口序号。
2. 例如，USG2200 的 slot1 和 slot5 分别安装了 5FE-SW 电接口卡和 2CE1 接口卡，那么接口的排列顺序如下：

   5FE-SW 电接口卡从左到右的 Ethernet 接口编号：Ethernet1/0/0、Ethernet 1/0/1、Ethernet 1/0/2、Ethernet 1/0/3、Ethernet 1/0/4。2CE1 接口卡从左到右接口编号为：controller e1 5/0/0、e1 5/0/1。主板 GE Combo 接口从左到右接口编号为：GigabitEthernet 0/0/0、GigabitEthernet0/0/1。

1.2.2 USG5100 产品描述

1.2.2.1 USG5120 产品外观

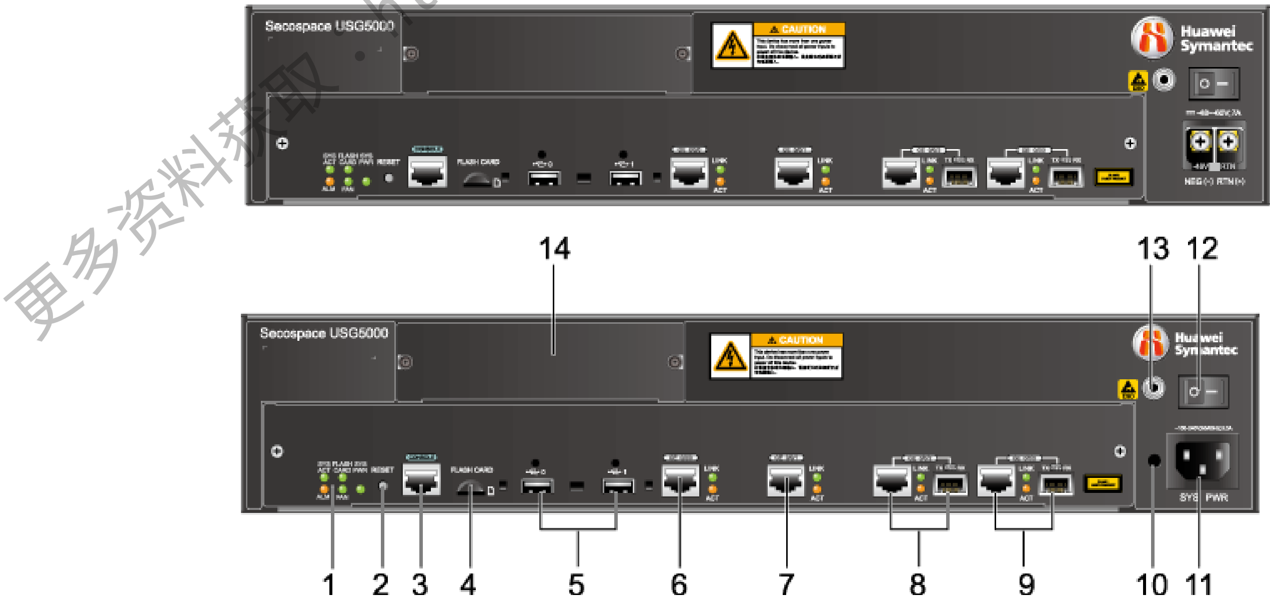
USG5150 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×130.5mm（宽×深×高），可以安装在 19 英寸标准机柜中。

1.2.2.2 USG5120 部件分布

前面板

USG5120 有交流和直流两种机型。

Figure 1-6 USG5120 产品前面板

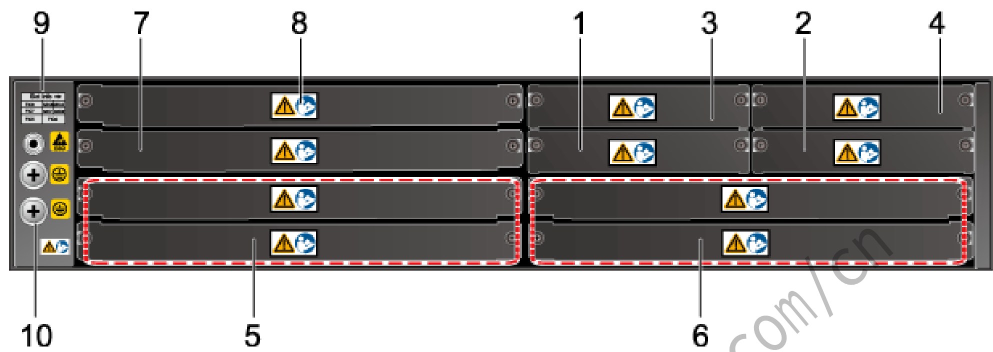


1.指示灯	2. 复位键	3.Console 接口	4.闪存接口
5.USB2.0 接口	6. 10/100/1000M 以太网接口 0	7.10/100/1000M 以太网接口 1	8.GE Combo 接口 2
9.GE Combo 接口 3	10.卡扣插孔	11.交流/直流电源插座	12.交流/直流电源开关

13.防静电手腕带插孔	14.防尘面板		

后面板

Figure 1-7 USG5120BSR 产品后面板



1. MIC1 插槽	2. MIC2 插槽	3. MIC3 插槽
4. MIC4 插槽	5. FIC5/DFIC5 插槽	6. FIC6/DFIC6 插槽
7. FIC7/DFIC7 插槽	8. FIC8 插槽	9. 槽位标识
10. 接地端子		

1.2.2.3 USG5150 产品外观

USG5150 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为442mm×414mm×130.5mm（宽×深×高），可以安装在 19 英寸标准机柜中。

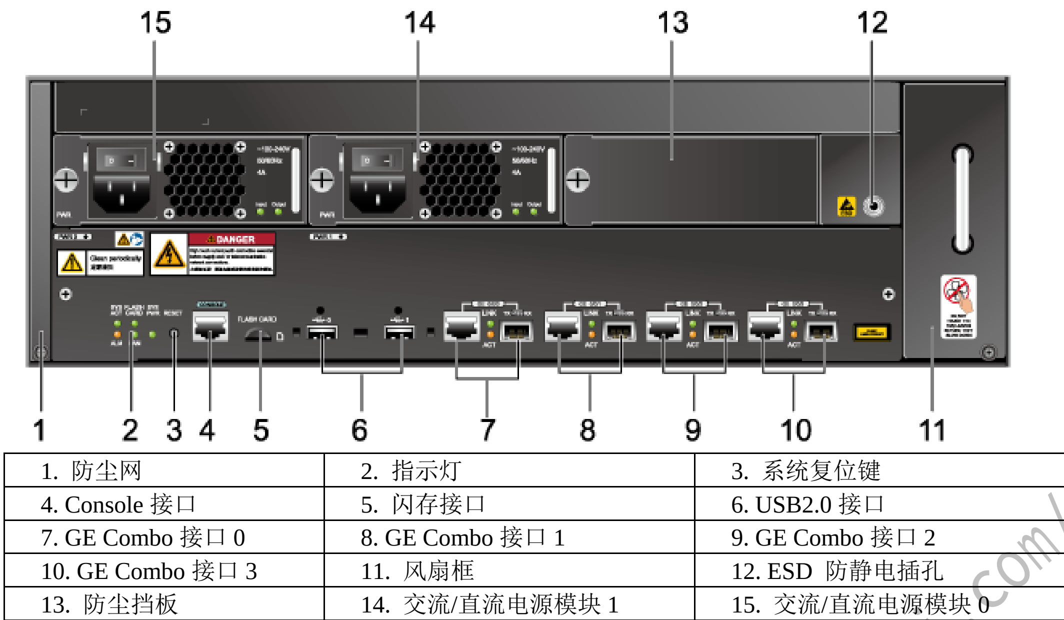
1.2.2.4 USG5150 部件分布

前面板

USG5150 的电源和风扇模块均可热插拔。

Figure 1-8 USG5150 产品前面板

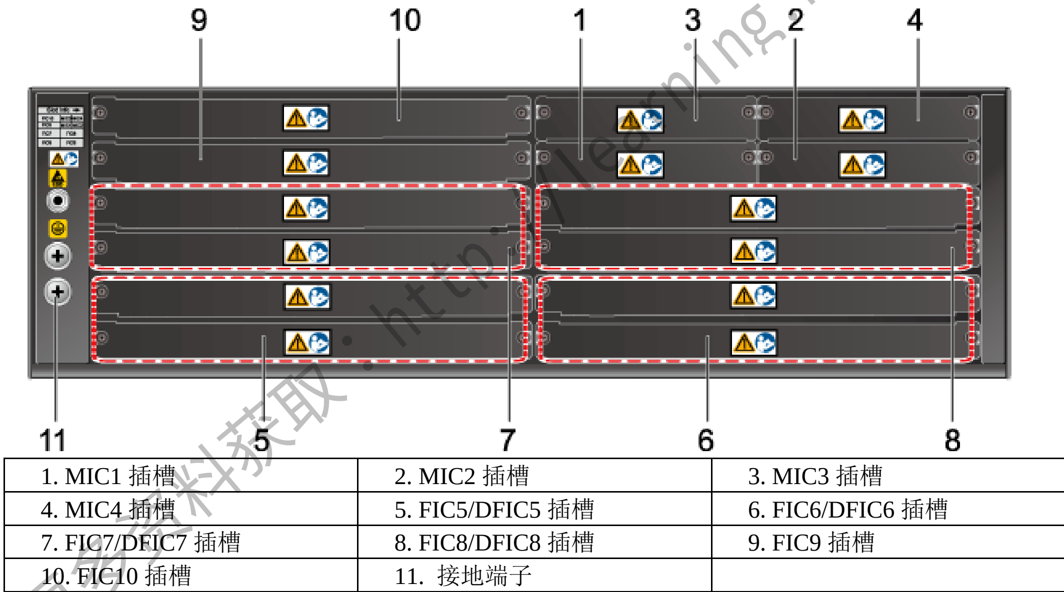




1. 防尘网	2. 指示灯	3. 系统复位键
4. Console 接口	5. 闪存接口	6. USB2.0 接口
7. GE Combo 接口 0	8. GE Combo 接口 1	9. GE Combo 接口 2
10. GE Combo 接口 3	11. 风扇框	12. ESD 防静电插孔
13. 防尘挡板	14. 交流/直流电源模块 1	15. 交流/直流电源模块 0

后面板

Figure 1-9 USG5150 产品后面板



1. MIC1 插槽	2. MIC2 插槽	3. MIC3 插槽
4. MIC4 插槽	5. FIC5/DFIC5 插槽	6. FIC6/DFIC6 插槽
7. FIC7/DFIC7 插槽	8. FIC8/DFIC8 插槽	9. FIC9 插槽
10. FIC10 插槽	11. 接地端子	

1.2.3 USG5500 产品描述

1.2.3.1 USG5530S 产品外观

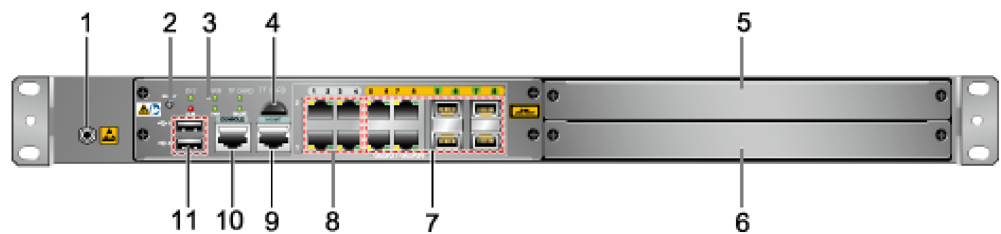
USG5530S 由一体化机箱、扩展接口卡组成。设备的一体化机箱尺寸为 442mm×560mm×43.6mm（宽×深×高），可以安装在 19 英寸标准机柜中。

1.2.3.2 USG5530S 部件分布

接口卡侧面板

如下图所示，USG5530S 支持 2 个 FIC 接口卡扩展插槽。

Figure 1-10 USG5530S 产品接口卡侧面板图

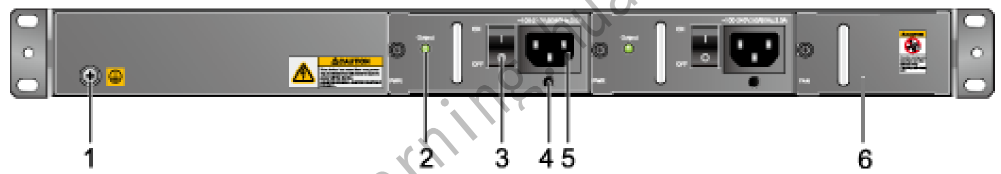


1. 防静电手腕带插孔	2. 系统复位键	3. 指示灯区域
4. Micro-SD 卡插槽	5. FIC2 插槽	6. 管理口
7. 光电互斥接口	8. 10/100/1000M 自适应以太网电接口	9. 管理口
10. Console 接口	11. USB 2.0 接口	

电源侧面板

如下图所示，USG5530S 只有交流机型，没有直流机型。

Figure 1-11 USG5530S 产品交流机型电源侧面板图



1. 接地端子	2. 电源指示灯	3. 电源开关
4. 交流电源线扎线孔	5. 电源接口	6. 风扇框

1.2.3.3 USG5530/5550/5560 产品外观

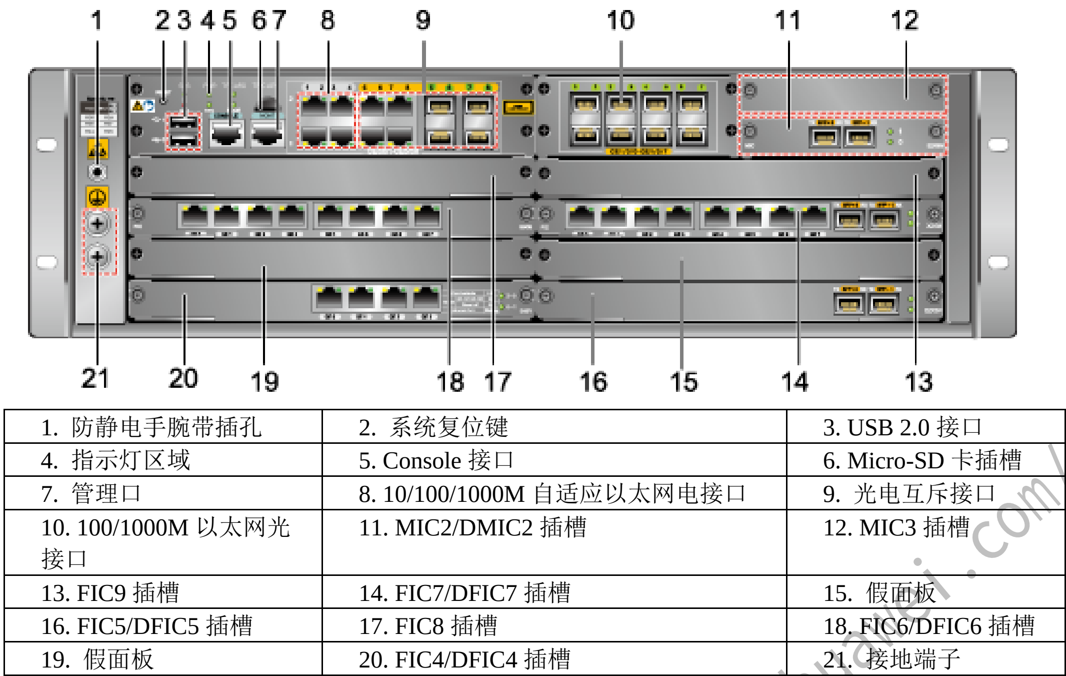
USG5530/5550/5560 由一体化机箱、扩展接口卡组成。USG5530/5550/5560 的一体化机箱尺寸为 442mm×414.1mm×130.5mm（宽×深×高），可以安装在 19 英寸标准机柜中。

1.2.3.4 USG5530/5550/5560 部件分布

接口卡侧面板

如下图所示，USG5530/5550/5560 支持 6 个 FIC 接口卡扩展插槽和 2 个 MIC 接口卡扩展插槽。其中，6 个 FIC 接口卡扩展插槽可合并为 4 个 DFIC 接口卡扩展插槽，2 个 MIC 接口卡扩展插槽可合并为 1 个 DMIC 接口卡扩展插槽。USG5530/5550/5560 暂不支持 MIC 和 DFIC 接口卡。

Figure 1-12 USG5530/5550/5560 产品接口卡侧面板图



1. 防静电手腕带插孔	2. 系统复位键	3. USB 2.0 接口
4. 指示灯区域	5. Console 接口	6. Micro-SD 卡插槽
7. 管理口	8. 10/100/1000M 自适应以太网电接口	9. 光电互斥接口
10. 100/1000M 以太网光接口	11. MIC2/DMIC2 插槽	12. MIC3 插槽
13. FIC9 插槽	14. FIC7/DFIC7 插槽	15. 假面板
16. FIC5/DFIC5 插槽	17. FIC8 插槽	18. FIC6/DFIC6 插槽
19. 假面板	20. FIC4/DFIC4 插槽	21. 接地端子

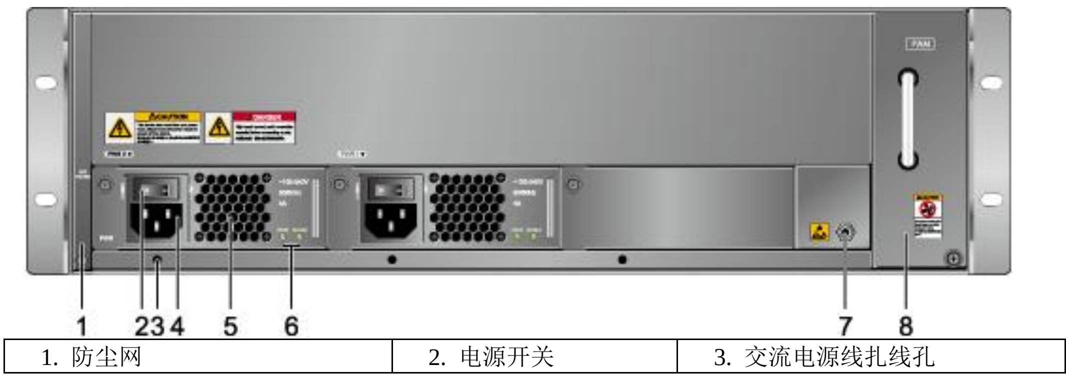
电源侧面板

如下图所示，USG5530 没有直流机型，只有交流机型；USG5550/5560 具有直流和交流两种机型。USG5550/5560 的直流机型和交流机型整机采用相同面板，直流机型的"3"号孔无需使用。

Figure 1-13 USG5550/5560 直流机型电源侧面板图



Figure 1-14 USG5530/5550/5560 交流机型电源侧面板图



1. 防尘网	2. 电源开关	3. 交流电源线扎线孔

4. 电源接口	5. 电源风扇网	6. 电源指示灯
7. 防静电手腕带插孔	8. 风扇框	

1.2.4 USG9500 产品描述

1.2.4.1 USG9500 产品外观

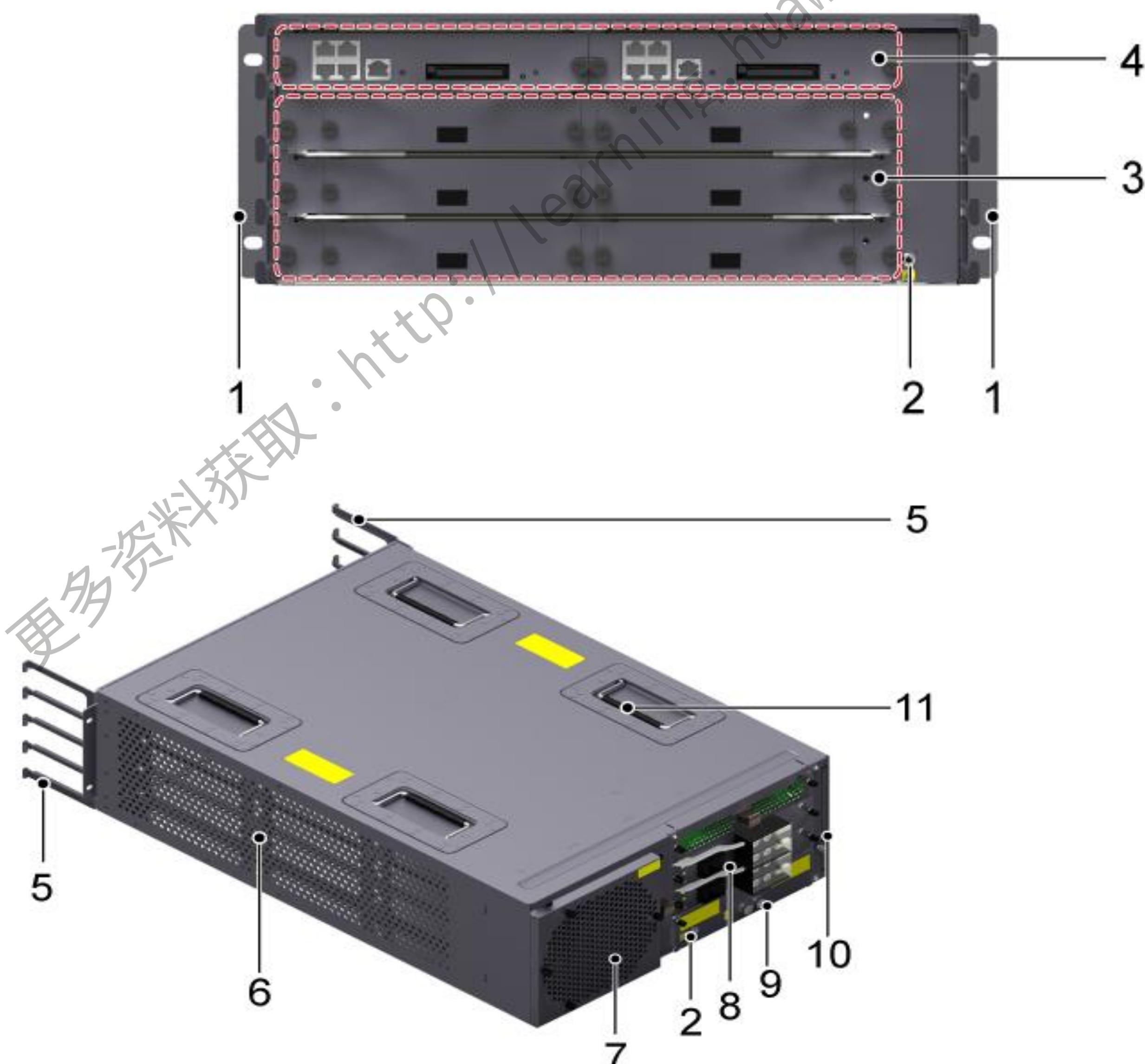
USG9000 系列产品都采用一体化机箱，可安装在 N68E-22 机柜或深度不小于 800mm 的 IEC（International Electrotechnical Commission）19 英寸标准机柜中。USG9000 产品外观如下图所示。

1.2.4.2 USG9520 部件分布

USG9520 有直流和交流两种相箱。

USG9520 直流机箱

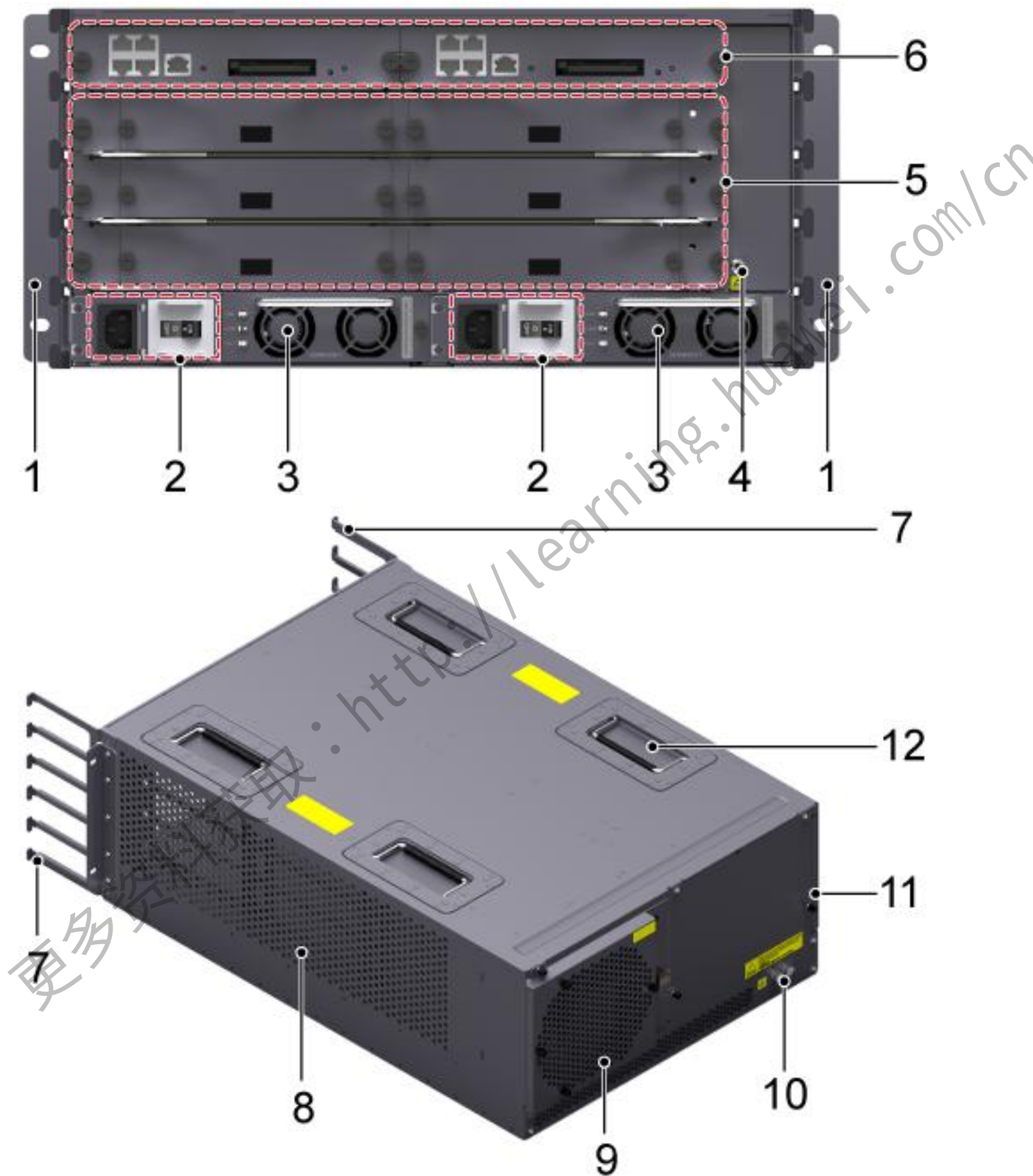
Figure 1-15 USG9520 直流机箱组成部件图



1. 挂耳	2. ESD 防静电插孔	3. LPU 槽位
4. MPU 槽位	5. 走线架	6. 进风口
7. 风扇	8. 直流电源模块	9. 保护接地端子
10. 防尘网	11. 把手	

USG9520 交流机箱

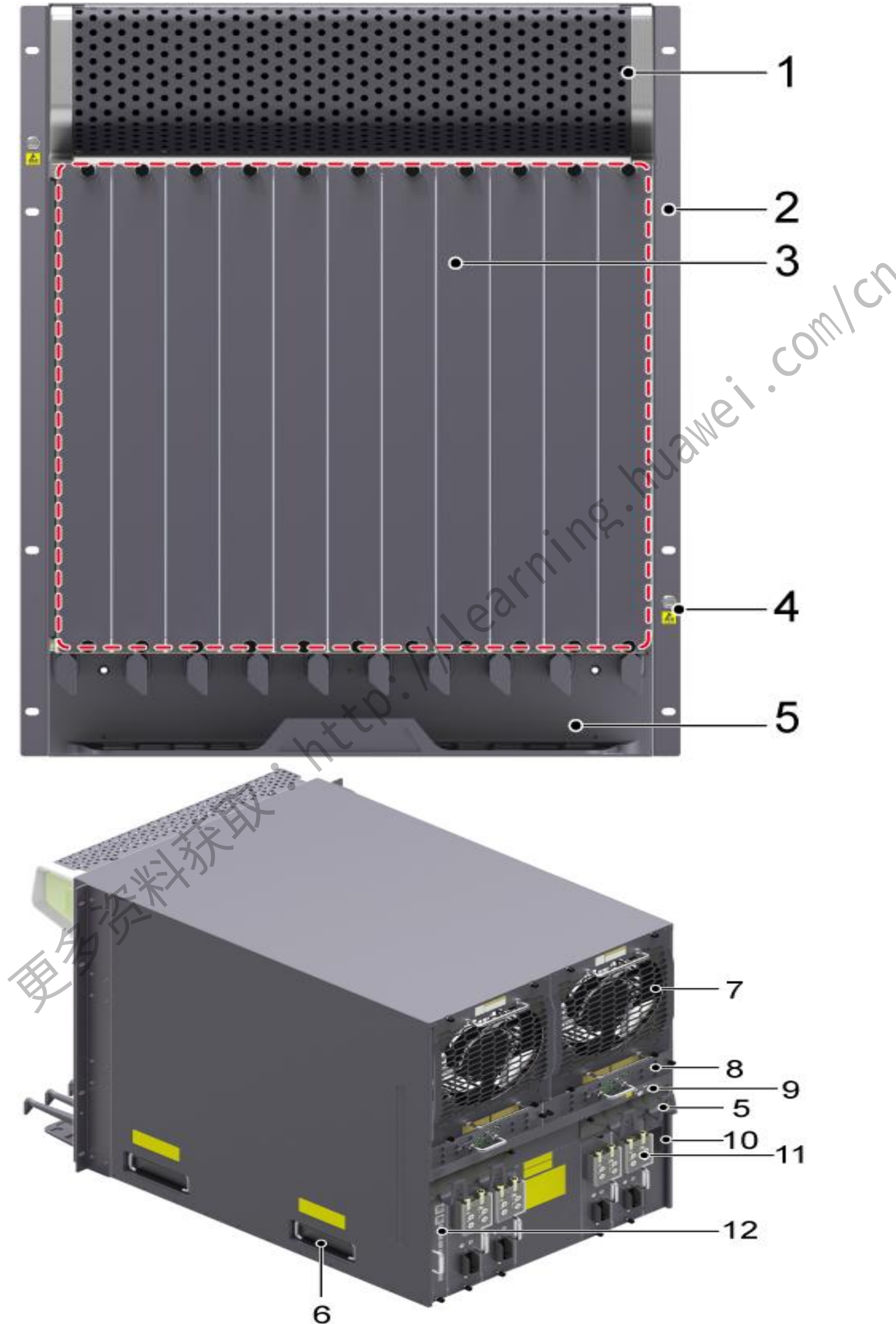
Figure 1-16 USG9520 交流机箱组成部件图



1. 挂耳	2. 电源开关和交流输入插座	3. 交流电源模块
4. ESD 防静电插孔	5. LPU 槽位	6. MPU 槽位
7. 走线架	8. 进风口	9. 风扇
10. 保护接地端子	11. 防尘网	12. 把手

1.2.4.3 USG9560 部件分布

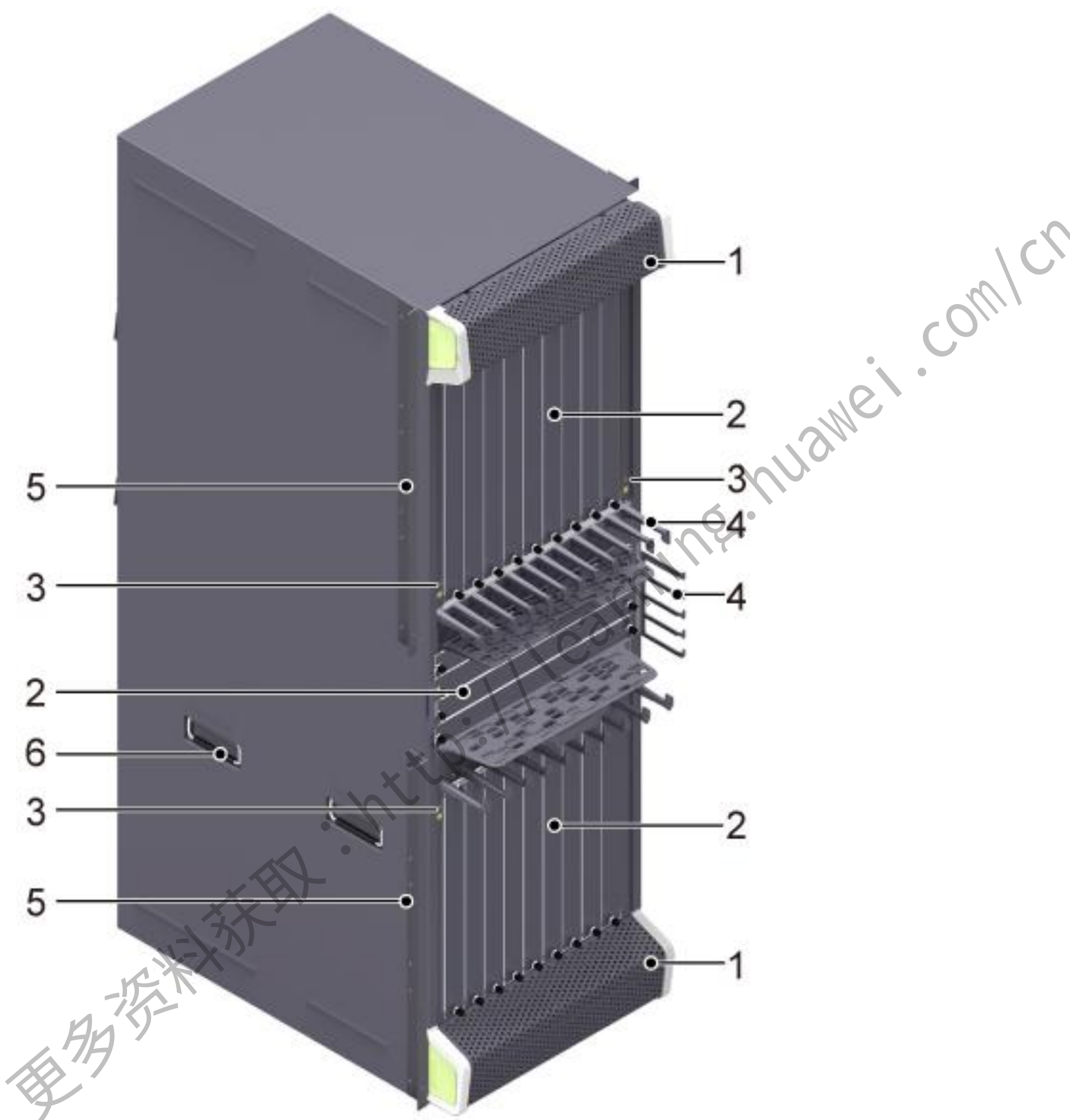
Figure 1-17 USG9560 部件图

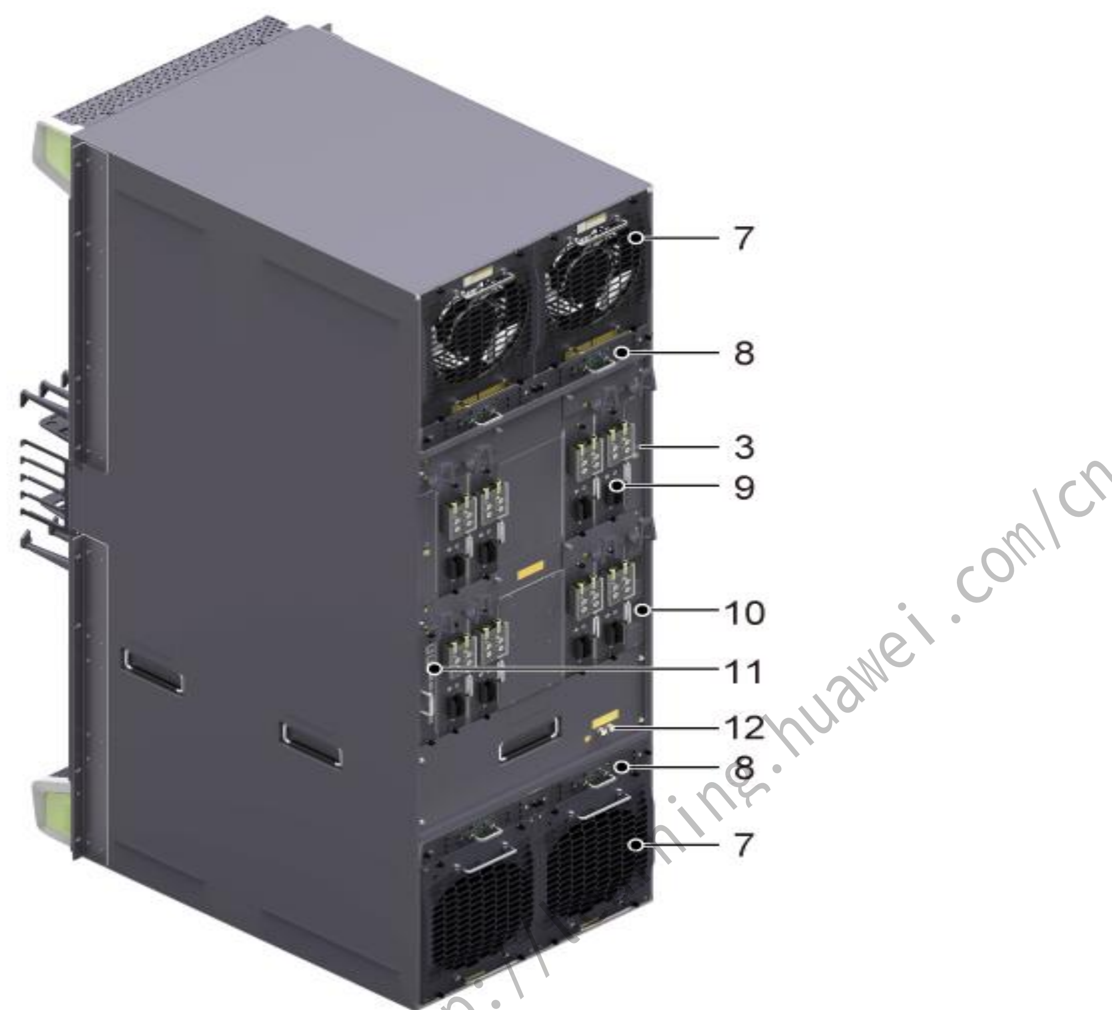


1. 进风口	2. 挂耳	3. 单板槽位区

4. ESD 插孔	5. 走线槽	6. 把手
7. 风扇	8. 电源滤波模块	9. 保护接地端子
10. 交流电源管理接口	11. PEM 模块	12. 集中监控模块

1.2.4.4 USG9580 部件分布





1. 进风口	2. 单板槽位区	3. ESD 插孔
4. 走线槽	5. 挂耳	6. 把手
7. 风扇模块	8. 电源滤波模块	9. PEM 模块
10. 交流电源管理接口	11. 集中监控模块	12. 保护接地端子

1.3 图示



2 防火墙高级设备管理

2.1 文件管理实验

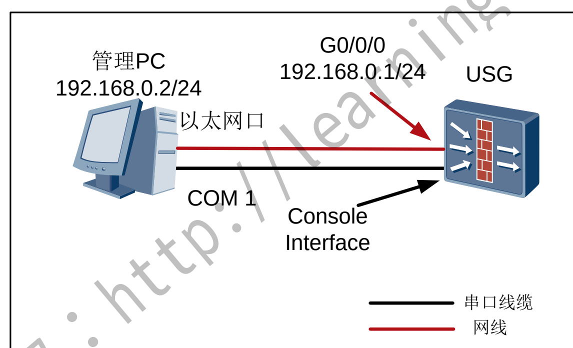
实验目的

学会查看设备中的文件，并配置 USG 为 FTP server

组网设备

PC 机一台，USG 防火墙一台。

实验拓扑图



实验步骤(命令行)

Setp 1 配置网络连接、IP 地址、接口安全区域及包过滤。（具体过程省略）

Setp 2 开启设备的 FTP 功能并配置 FTP 用户名、密码及 FTP 路径。

```
<USG> system-view
[USG] ftp server enable
Info:Start FTP server
[USG] aaa
[USG -aaa] local-user ftpuser password cipher Ftppass#
[USG -aaa] local-user ftpuser service-type ftp
[USG -aaa] local-user ftpuser level 3
[USG -aaa] local-user ftpuser ftp-directory hda1:/
```

Setp 3 从配置终端使用 ftp 命令登录到设备上。

备份文件管理：

使用 **get** 命令从设备下载文件到 PC。

这里以安装 Windows 操作系统的 PC 为例:“开始 > 运行”,输入 **cmd** 后单击“确定”。

```
C:\Documents and Settings\Administrator> ftp 192.168.0.1
Connected to 192.168.0.1.
220 FTP service ready.
User (192.168.0.1:(none)): ftpuser
331 Password required for ftpuser.
Password:
230 User logged in.
ftp> get vrpcfg.cfg
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.cfg.
226 Transfer complete.
ftp: 收到 5203 字节，用时 0.01Seconds 346.87Kbytes/sec.
ftp> lcd
Local directory now C:\Documents and Settings\Administrator.
ftp>
```

恢复文件：

恢复的步骤和备份的步骤类似，但是有两点不同点。

//恢复使用 **put** 命令将文件上传到设备上。

```
ftp> put vrpcfg.cfg
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.cfg.
226 Transfer complete.
ftp: 发送 5203 字节，用时 0.00Seconds 5203000.00Kbytes/sec.
```

// **在 USG 设备中配置命令行**，配置设备下次启动使用的配置文件。

```
<USG> startup saved-configuration vrpcfg.cfg
```

验证结果

查看上传及下载文件时是否成功。

2.2 AAA方式设备管理

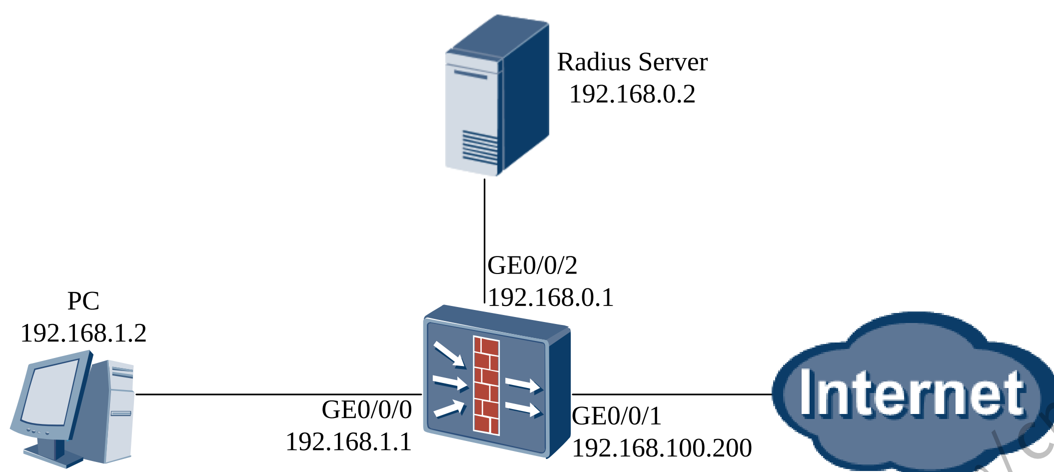
实验目的

采用 Radius 服务器验证方式对用户进行认证，用户认证通过后，可接入互联网。

组网设备

PC 机一台，USG 系列防火墙一台，装有 Radius 服务的 PC 机一台。

实验拓扑图



验步骤(命令行)

Setp 1 配置各接口 IP 地址，并将各接口加入相应安全区域。

```
[USG2200]int GigabitEthernet 0/0/0
[USG2200-GigabitEthernet0/0/0]ip address 192.168. 1.1 24
[USG2200-GigabitEthernet0/0/0]quit
[USG2200]firewall zone trust
[USG2200-zone-dmz]add interface GigabitEthernet 0/0/0
[USG2200-zone-dmz]quit
[USG2200]int GigabitEthernet 0/0/1
[USG2200-GigabitEthernet0/0/1]ip address 192.168.100.200 24
[USG2200-GigabitEthernet0/0/1]quit
[USG2200]firewall zone untrust
[USG2200-zone-untrust]add interface GigabitEthernet 0/0/1
[USG2200-zone-untrust]quit
[USG2200]int GigabitEthernet 0/0/2
[USG2200-GigabitEthernet0/0/2]ip address 192.168. 0.1 24
[USG2200-GigabitEthernet0/0/2]quit
[USG2200]firewall zone dmz
[USG2200-zone-dmz]add interface GigabitEthernet 0/0/2
[USG2200-zone-dmz]quit
```

Setp 2 配置域间转发策略，保证网络连通性。

```
[USG2200]firewall packet-filter default permit interzone trust untrust
[USG2200]firewall packet-filter default permit interzone trust dmz
[USG2200]firewall packet-filter default permit interzone dmz untrust
```

Setp 3 配置路由，使防火墙可以与互联网进行通信。

```
[USG2200]ip route-static 0.0.0.0 0.0.0.0 192.168.100.254
```

Setp 4 配置 NAT 策略。

```
[USG2200]nat-policy interzone untrust trust outbound
[USG2200-nat-policy-interzone-trust-untrust-outbound]policy 0
[USG2200-nat-policy-interzone-trust-untrust-outbound-0]action source-nat
[USG2200-nat-policy-interzone-trust-untrust-outbound-0]policy source 192.168.1.0 0.0.0.255
[USG2200-nat-policy-interzone-trust-untrust-outbound-0]easy-ip GigabitEthernet 0/0/1
```

Setp 5 配置 DNS 服务器，保证内网用户可以链接上互联网。

```
[USG2200]dns server 210.21.196.6
```

Setp 6 配置 Radius 服务器

```
[USG2200]radius-server template 1
Info: Succeeded in Creating a new server template.
[USG2200-radius-1]radius-server authentication 192.168.0.2 1812
[USG2200-radius-1]radius-server accounting 192.168.0.2 1813
[USG2200-radius-1]radius-server shared-key 12345
```

测试 USG 与 RADIUS 服务器的连通性。此处的测试用户名和密码需要与 RADIUS 服务器上已经存在的账号的用户名和密码保持一致。

```
[USG2200-radius-1]radius-server test user test test
```

Setp 7 配置用户信息。（此处创建的用户名及用户组需要与 radius server 上以后的用户名和用户组保持一致。）

创建名为 Jason 的用户。

```
[USG2200] user-manage user Jason
```

创建名为 admin 的用户组，并将用户名为 Jason 的用户加入该用户组。

```
[USG2200-localuser-Jason] user-manage group /admin
```

Setp 8 配置认证策略。策略名为 Radius_Policy。

```
[USG2200]user-manage authentication-policy Radius_Policy
[USG2200-authpolicy-radius_policy]authentication-mode password radius template 1
[USG2200-authpolicy-radius_policy]ip-range 192.168.1.2 192.168.1.10
[USG2200-authpolicy-radius_policy]quit
```


实验步骤(Web)

Setp 1 配置各接口 IP 地址，并将各接口加入相应安全区域。（略）

Setp 2 配置域间转发策略，保证网络连通性。选择**防火墙>安全策略>转发策略**，在 trust 到 untrust 区域的策略项后单击，修改策略为“permit”。配置完成后单击“**应用**”。

防火墙 > 安全策略 > 转发策略

修改转发策略

源安全区域	trust *
目的安全区域	untrust *
源地址	any
目的地址	any
用户	请选择或输入用户或用户组
服务	请选择服务
时间段	all
动作	permit *

应用 返回

Setp 3 配置路由，使防火墙可以与互联网进行通信。选择**路由>静态>静态路由**，单击“**新建**”，添加一条静态路由。配置完成后单击“**应用**”。

路由 > 静态 > 静态路由

新建静态路由

目的地址	0 . 0 . 0 . 0 *
掩码	0 . 0 . 0 . 0 *
下一跳	192 . 168 . 100 . 254 下一跳和接口不能同时为空
接口	----- NONE -----
IP Link号	----- NONE -----
优先级	60 <1-255>

应用 返回

Setp 4 配置 NAT 策略。选择**防火墙>NAT>源 NAT**，单击“**新建**”，选择将源地址转换为接口 IP 地址，接口为连接互联网的出接口（GE0/0/1）。配置完成后单击“**应用**”。

防火墙 > NAT > 源NAT

源NAT | NAT地址池

新建源NAT

源安全区域	trust *
目的安全区域	untrust *
源地址	192.168.0.0/24 多选
目的地址	请选择或输入IP地址 多选
动作	NAT转换 *
描述	
将源地址转换为	○ 地址池中的地址 ● 接口IP地址
接口	GE0/0/1 *

应用 返回

Setp 5 配置 DNS 服务器，保证内网用户可以链接上互联网。选择**网络>DNS>DNS**，在**服务器列表**中输入 DNS 服务器地址，单击“**添加**”。

网络 > DNS > DNS

服务器列表

删除 刷新 | 添加

IP	获取方式
210.21.196.6	STATIC

Setp 6 配置 Radius 服务器。选择**用户>认证服务器>RADIUS 服务器**，单击列表中的**新建**，创建一个 radius 服务器。设置共享密码为 123456。配置完成后单击“**应用**”。

用户 > 认证服务器 > RADIUS服务器

修改RADIUS服务器

RADIUS服务器名称	1 *	共享密钥	••••••••••••••••••••
认证主服务器IP	192 . 168 . 0 . 2	端口	1812 <1-65535>
认证从服务器IP	. . .	端口	1812 <1-65535>
计费主服务器IP	192 . 168 . 0 . 2	端口	1813 <1-65535>
计费从服务器IP	. . .	端口	1813 <1-65535>

高级选项

重传次数	3	字节格式	Byte
应答超时时间	5 秒	服务器类型	◉ 标准 ○ Portal
NAS-Port端口类型	○ 旧 ◉ 新	NAS-Port-Id端口类型	○ 旧 ◉ 新
计费停止报文重传	☐ 启用		
用户名格式	☐ 包含用户组名称		

应用　返回

测试 USG 与 RADIUS 服务器的连通性。点击配置下的 图标。测试成功后将会看到如下提示：



Setp 7 配置用户信息。（此处创建的用户名及用户组需要与 radius server 上以后的用户名和用户组保持一致。）

创建名为 admin 的用户组。选择**用户>上网用户>组/用户**，单击**新建**，选择**新建组**，输入组名，单击“**应用**”。



用户 > 上网用户 > 组/用户

新建组

组名 admin *

描述

所属组 root 选择

应用 返回

\# 创建名为 Jason 的用户。单击**新建**，选择**新建用户**，输入用户名，选择所属组为 admin。单击“**应用**”。



用户 > 上网用户 > 组/用户

新建用户

登录名 Jason *

显示名

描述

所属组 root,/admin 选择

本地密码

用户属性

应用 返回

Setp 8 配置认证策略。策略名为 Radius_Policy。选择**用户>上网用户>认证策略**，单击**新建**，创建**认证策略**。选择认证方式为**本地密码认证/服务器认证**，认证服务器类型为 **RADIUS**，认证服务器名称为 **1**。单击**应用**。

用户 > 上网用户 > 认证策略

新建认证策略

名称 Radius_Policy *

描述

IP地址范围1 *

认证方式 本地密码认证/服务器认证

认证服务器类型 RADIUS LDAP AD

认证服务器名称 1

新用户认证选项（新用户指本地不存在的账户）

应用 返回

验证结果

配置完成后，用户使用浏览器上网时将会弹出验证对话框，输入用户名密码后，即可上网。

2.3 BootRoom 密码恢复

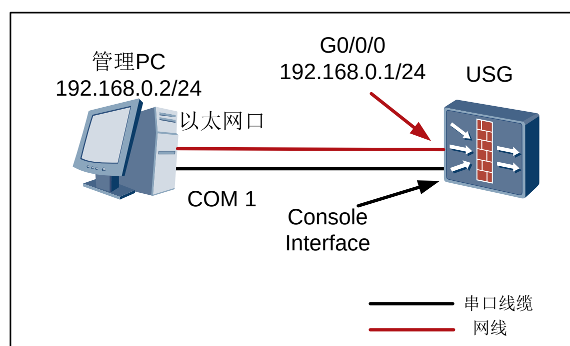
实验目的

在 BootROM 中配置跳过 Console 口密码登录后，重新进行设置。部分设备的 BootROM 提供了清空 Console 口密码的功能，可以在用户使用 Console 口登录的时候跳过用户名密码检查。这样系统启动后除了不需要输入 console 密码外，与正常启动相同，也会完成所有配置加载。

组网设备

PC 机一台，USG 系列防火墙一台。

实验拓扑图



实验步骤(命令行)

Setp 1 连接到设备 console 接口。

Setp 2 重启设备，出现“Press Ctrl+B to Enter Boot Menu...”打印信息时，按下“Ctrl+B”并键入密码“O&m15213”后进入 BootROM 主菜单。

Setp 3 在主菜单中或隐藏菜单（主菜单中按 Ctrl+z 进入）中选择“Recover Console Password”对应序号。

说明：

部分设备显示为“Skip Console0 Password”，该选项功能作用与“Recover Console Password”作用相同。

Setp 4 如果主菜单和隐藏菜单均没有类似选项，则说明设备不支持跳过 Console 口密码登录，请选择其他方法解决。

Setp 5 在主菜单中选择“Reboot”重新启动。

Setp 6 进入系统后，以配置 Console 口用户名 admin、密码为 Admin@123 为例。

```
<USG> system-view
[USG] user-interface console 0
[USG -ui-console0] authentication-mode local user admin password cipher
Admin@123
[USG -ui-console0] return
```

Setp 7 保存修改，重启后可以使用新的用户名和密码登录。

```
< USG > save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the device............................
...........................
Info:The current configuration was saved to the device successfully.
```

实验步骤(Web)

N/A

验证结果

使用新创建的用户名和密码登陆设备成功。

3 防火墙高级安全特性

3.1 基于IP地址连接数限制和带宽限制

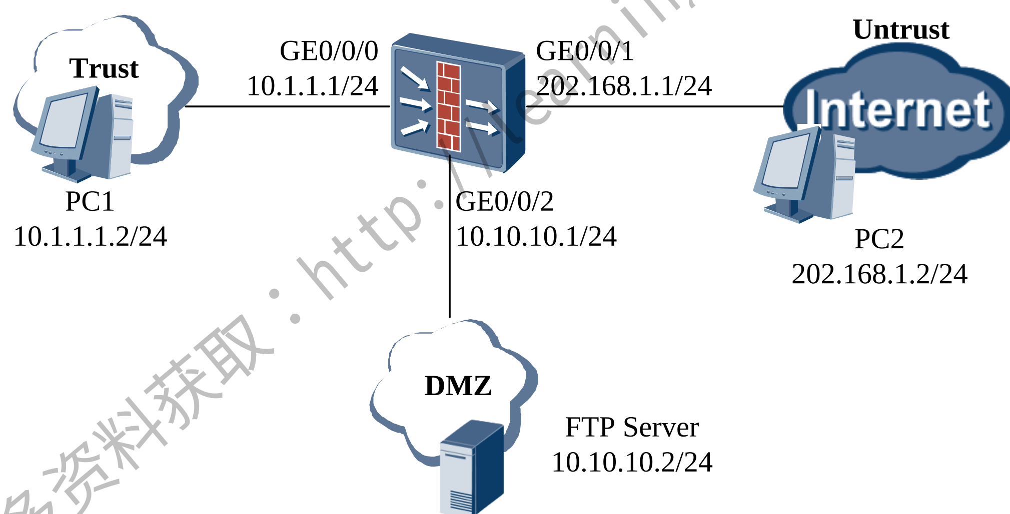
实验目的

了解到基于 IP 地址的连接数限制和带宽限制典型组网和配制方法。

组网设备

PC 机 3 台、USG 5000 系列防火墙 1 台

实验拓扑图



具体需求如下：

- 为防止 FTP 服务器受攻击，限制从 Trust 区域和 Untrust 区域到 FTP 端口的连接数上限为 20，并且限制其上传/下载带宽为：5Mbps/10Mbps。
- 限制 Trust 域内每个 PC 用户到 internet 的上传/下载带宽为：400kbps/600kbps。

实验步骤（CLI）

Setp 1 配置 USG 基本数据。

\# 配置 USG 接口 IP 地址。

```
<USG> system-view
```

```
[USG] interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0] ip address 10.1.1.1 24
[USG-GigabitEthernet0/0/0] quit
[USG] interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1] ip address 20.1.1.1 24
[USG-GigabitEthernet0/0/1] quit
[USG] interface GigabitEthernet 0/0/2
[USG-GigabitEthernet0/0/2] ip address 10.10.10.1 24
[USG-GigabitEthernet0/0/2] quit
```

将 USG 各接口加入域。

```
[USG] firewall zone trust
[USG-zone-trust] add interface GigabitEthernet 0/0/0
[USG-zone-trust] quit
[USG] firewall zone dmz
[USG-zone-dmz] add interface GigabitEthernet 0/0/2
[USG-zone-dmz] quit
[USG] firewall zone untrust
[USG-zone-untrust] add interface GigabitEthernet 0/0/1
[USG-zone-untrust] quit
```

Setp 2 配置域间防火墙策略。

通过配置域间防火墙策略满足如下两个需求：

- Trust 域和 Untrust 域的用户可以访问 DMZ 域的 FTP 服务器。
- Trust 域用户可以访问 Untrust 域。

```
[USG] policy interzone trust untrust outbound
[USG-policy-interzone-trust-untrust-outbound] policy 1
[USG-policy-interzone-trust-untrust-outbound-1] policy source 10.1.1.0 mask 24
[USG-policy-interzone-trust-untrust-outbound-1] action permit
[USG-policy-interzone-trust-untrust-outbound-1] quit
[USG-policy-interzone-trust-untrust-outbound] quit
[USG] policy interzone trust dmz outbound
[USG-policy-interzone-trust-dmz-outbound] policy 1
[USG-policy-interzone-trust-dmz-outbound-1] policy source 10.1.10.0 mask 24
[USG-policy-interzone-trust-dmz-outbound-1] policy destination 10.10.10.2 0
[USG-policy-interzone-trust-dmz-outbound-1] policy service service-set ftp
[USG-policy-interzone-trust-dmz-outbound-1] action permit
[USG-policy-interzone-trust-dmz-outbound-1] quit
[USG-policy-interzone-trust-dmz-outbound] quit
```

```
[USG] policy interzone untrust dmz inbound
[USG-policy-interzone-dmz-untrust-inbound] policy 2
[USG-policy-interzone-dmz-untrust-inbound-2] policy destination 10.10.10.2 0
[USG-policy-interzone-dmz-untrust-inbound-2] policy service service-set ftp
[USG-policy-interzone-dmz-untrust-inbound-2] action permit
[USG-policy-interzone-dmz-untrust-inbound-2] quit
[USG-policy-interzone-dmz-untrust-inbound] quit
```

Setp 3 配置 NAT 策略。

```
[USG] nat address-group 1 202.168.1.10 202.168.1.20
[USG] nat-policy interzone trust untrust outbound
[USG-nat-policy-interzone-trust-untrust-outbound] policy 1
[USG-nat-policy-interzone-trust-untrust-outbound-1] policy source 10.1.1.0 mask 24
[USG-nat-policy-interzone-trust-untrust-outbound-1] action source-nat
[USG-nat-policy-interzone-trust-untrust-outbound-1] address-group 1
[USG-nat-policy-interzone-trust-untrust-outbound-1] quit
[USG-nat-policy-interzone-trust-untrust-outbound] quit
```

Setp 4 配置内部服务器。

```
[USG] nat server protocol tcp global 202.168.1.100 ftp inside 10.10.10.2 ftp
[USG] firewall interzone trust dmz
[USG-interzone-trust-dmz] detect ftp
[USG-interzone-trust-dmz] quit
[USG] firewall interzone dmz untrust
[USG-interzone-dmz-untrust] detect ftp
[USG-interzone-dmz-untrust] quit
```

Setp 5 启用限流策略功能。

```
[USG]traffic-policy enable
```

Setp 6 启用 DPI 应用控制功能，使 DPI 应用协议能配限流策略应用，实现对应用协议的限流。

```
[USG] dpi enable
Info: Initialize DPI, please wait......................................................
[USG]
```

Setp 7 配置 FTP 服务器的连接数限制和带宽限制。

配置从 trust 和 untrust 区域到 DMZ 区域的 FTP 连接数限制上限为 20。

```
[USG] car-class class1 type shared
[USG-shared-car-class-class1] connection-number 20
```

```
[USG-shared-car-class-class1] quit
[USG] traffic-policy interzone dmz untrust inbound shared
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared] policy 1
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared-1] policy car-class class1
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared-1] policy destination
10.10.10.0 0.0.0.255
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared-1] policy service
service-set ftp
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared-1] action car
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared-1] quit
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared] quit
[USG] traffic-policy interzone dmz trust outbound shared
[USG-traffic-policy-interzone-trust-dmz-outbound-shared] policy 1
[USG-traffic-policy-interzone-trust-dmz-outbound-shared-1] policy car-class class1
[USG-traffic-policy-interzone-trust-dmz-outbound-shared-1] policy destination
10.10.10.0 0.0.0.255
[USG-traffic-policy-interzone-trust-dmz-outbound-shared-1] policy service
service-set ftp
[USG-traffic-policy-interzone-trust-dmz-outbound-shared-1] action car
[USG-traffic-policy-interzone-trust-dmz-outbound-shared-1] quit
[USG-traffic-policy-interzone-trust-dmz-outbound-shared] quit
```

配置从 trust 区域和 untrust 区域到 DMZ 区域 FTP 服务器的上传带宽限制为 5Mbps。

```
[USG] car-class class2 type shared
[USG-shared-car-class-class2] car 5000
[USG-shared-car-class-class2] quit
[USG] traffic-policy interzone dmz trust outbound shared
[USG-traffic-policy-interzone-trust-dmz-outbound-shared] policy 2
[USG-traffic-policy-interzone-trust-dmz-outbound-shared-2] policy car-class class2
[USG-traffic-policy-interzone-trust-dmz-outbound-shared-2] action car
[USG-traffic-policy-interzone-trust-dmz-outbound-shared-2] policy destination
10.10.10.0 0.0.0.255
[USG-traffic-policy-interzone-trust-dmz-outbound-shared-2] policy service
service-set ftp
[USG-traffic-policy-interzone-trust-dmz-outbound-shared-2] quit
[USG-traffic-policy-interzone-trust-dmz-outbound-shared] quit
[USG] traffic-policy interzone dmz untrust inbound shared
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared] policy 2
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared-2] action car
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared-2] policy car-class class2
```

```
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared-2] policy destination 10.10.10.0 0.0.0.255
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared-2] policy service service-set ftp
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared-2] quit
[USG-traffic-policy-interzone-dmz-untrust-inbound-shared] quit
```

配置从 trust 区域和 untrust 区域到 DMZ 区域 FTP 服务器的下载带宽限制为 10Mbps。

```
[USG] car-class class3 type shared
[USG-shared-car-class-class3] car 10000
[USG-shared-car-class-class3] quit
[USG] traffic-policy interzone dmz untrust outbound shared
[USG-traffic-policy-interzone-dmz-untrust-outbound-shared] policy 3
[USG-traffic-policy-interzone-dmz-untrust-outbound-shared-3] policy source 10.10.10.0 0.0.0.255
[USG-traffic-policy-interzone-dmz-untrust-outbound-shared-3] policy car-class class3
[USG-traffic-policy-interzone-dmz-untrust-outbound-shared-3] policy service service-set ftp
[USG-traffic-policy-interzone-dmz-untrust-outbound-shared-3] quit
[USG-traffic-policy-interzone-dmz-untrust-outbound-shared] quit
[USG] traffic-policy interzone dmz trust inbound shared
[USG-traffic-policy-interzone-trust-dmz-inbound-shared] policy 3
[USG-traffic-policy-interzone-trust-dmz-inbound-shared-3] action car
[USG-traffic-policy-interzone-trust-dmz-inbound-shared-3] policy source 10.10.10.0 0.0.0.255
[USG-traffic-policy-interzone-trust-dmz-inbound-shared-3] policy car-class class3
policy service service-set ftp
[USG-traffic-policy-interzone-trust-dmz-inbound-shared-3] quit
[USG-traffic-policy-interzone-trust-dmz-inbound-shared] quit
```

Setp 8 配置 PC 带宽限制。

在 Trust 到 Untrust 的 Outbound 方向上配置每 IP 限流策略 1，引用 car-class class4，限制上传最大带宽为 400kbps。

```
[USG] car-class class4 type per-ip
[USG-per-ip-car-class-class1] car max 400
[USG-per-ip-car-class-class1] quit
[USG] traffic-policy interzone trust untrust outbound per-ip
[USG-traffic-policy-interzone-trust-untrust-outbound-per-ip] policy 4
```

```
[USG-traffic-policy-interzone-trust-untrust-outbound-per-ip-4] policy car-type source-ip
[USG-traffic-policy-interzone-trust-untrust-outbound-per-ip-4] policy source 10.1.1.0 0.0.0.255
[USG-traffic-policy-interzone-trust-untrust-outbound-per-ip-4] policy car-class class4
[USG-traffic-policy-interzone-trust-untrust-outbound-per-ip-4] policy service service-set ftp
[USG-traffic-policy-interzone-trust-untrust-outbound-per-ip-4] action car
[USG-traffic-policy-interzone-trust-untrust-outbound-per-ip-4] quit
[USG-traffic-policy-interzone-trust-untrust-outbound-per-ip] quit
```

在 Trust 到 Untrust 的 inbound 方向上配置每 IP 限流策略 2，引用 car-class class5，限制 P2P 下载最大带宽为 600kbps。

```
[USG] car-class class5 type per-ip
[USG-per-ip-car-class-class2] car max 600
[USG-per-ip-car-class-class2] quit
[USG] traffic-policy interzone trust untrust inbound per-ip
[USG-traffic-policy-interzone-trust-untrust-inbound-per-ip] policy 5
[USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-5] policy car-type destination-ip
[USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-5] policy destination 10.1.1.0 0.0.0.255
[USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-5] policy car-class class5
[USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-5] policy service service-set ftp
[USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-5] policy category p2p
[USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-5] action car
[USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-5] quit
[USG-traffic-policy-interzone-trust-untrust-inbound-per-ip] quit
```


实验步骤（Web）

Setp 1 配置各接口 IP 地址并将其加入安全区域。（略）

Setp 2 配置包过滤策略，保证路由可达。

防火墙 > 安全策略 > 转发策略

转发策略列表

新建 删除 清除全部命中次数 刷新 | any zone --> any zone 查询 | 高级查询

ID	源地址	目的地址	用户	服务	时间段	动作
untrust->trust						
默认	any	any	any	ip	all	permit
trust->untrust						
默认	any	any	any	ip	all	permit
dmz->trust						
默认	any	any	any	ip	all	permit
trust->dmz						
默认	any	any	any	ip	all	permit
untrust->dmz						
默认	any	any	any	ip	all	permit
dmz->untrust						
默认	any	any	any	ip	all	permit

Setp 3 配置 NAT 策略。

创建 NAT 地址池 1。选择“**防火墙 > NAT > 源 NAT**”。选择“**NAT 地址池**”页签。

在“**NAT 地址池列表**”中单击，配置完成后单击“**应用**”。

防火墙 > NAT > 源NAT

源NAT | NAT地址池

新建NAT地址池

地址池号	1	*<0-1023>
地址池名称		
起始IP	202 . 168 . 1 . 10	*
结束IP	202 . 168 . 1 . 20	*

应用 返回

配置源 NAT。选择“**防火墙 > NAT > 源 NAT**”。选择“**源 NAT**”页签，在“**源 NAT 策略列表**”中单击，配置完成后单击“**应用**”。

Setp 4 配置 NAT server。选择“**防火墙 > NAT > 虚拟服务器**”，在“**虚拟服务器列表**”中单击 ，配置完成后单击“**应用**”。

Setp 5 启用限流策略。选择“**防火墙 > 限流策略 > 基本配置**”，选中“**限流策略**”对应的“**启用**”复选框，单击“**应用**”。



Setp 6 配置整体限流。配置 FTP 服务器的连接数限制和带宽限制。

创建整体限流 class。选择“**防火墙 > 限流策略 > 整体限流**”，选择“**整体限流 Class**”页签，单击，新建整体限流。

Class1 为 FTP 服务器最大连接数限制；Class2 为从 trust 区域和 untrust 区域到 DMZ 区域 FTP 服务器的上传带宽限制；class3 为从 trust 区域和 untrust 区域到 DMZ 区域 FTP 服务器的下载带宽限制。





防火墙 > 限流策略 > 整体限流

整体限流 | 整体限流Class

修改整体限流Class

名称	class3	*
最大带宽	10	<8-10000000>kbps
最大连接数		<1-1000000>

应用 返回

配置从 trust 和 untrust 区域到 DMZ 区域的 FTP 连接数限制，选择“**整体限流**”页签单击，新建整体限流策略 1，引用 class1。

防火墙 > 限流策略 > 整体限流

整体限流 | 整体限流Class

修改整体限流策略

源安全区域	trust	*
目的安全区域	dmz	*
源地址	any	多选
目的地址	10.10.10.0\0.0.0.255	多选
用户	any	多选
应用协议	请选择应用协议	多选
服务	ftp	多选
时间段	all	
动作	限流	*
描述		
整体限流Class	class1	*

防火墙 > 限流策略 > 整体限流

整体限流　整体限流Class

修改整体限流策略

字段	值
源安全区域	untrust
目的安全区域	dmz
源地址	any
目的地址	10.10.10.0\0.0.0.255
用户	any
应用协议	请选择应用协议
服务	ftp
时间段	all
动作	限流
描述	
整体限流Class	class1

\# 配置从 trust 区域和 untrust 区域到 DMZ 区域 FTP 服务器的上传带宽限制引用 class2。

防火墙 > 限流策略 > 整体限流

整体限流 | 整体限流Class

修改整体限流策略

源安全区域	trust *
目的安全区域	dmz *
源地址	any 多选
目的地址	10.10.10.0\0.0.0.255 多选
用户	any 多选
应用协议	请选择应用协议 多选
服务	ftp 多选
时间段	all
动作	限流 *
描述	
整体限流Class	class2 *

防火墙 > 限流策略 > 整体限流

整体限流 | 整体限流Class

修改整体限流策略

源安全区域	untrust *
目的安全区域	dmz *
源地址	any 多选
目的地址	10.10.10.0\0.0.0.255 多选
用户	any 多选
应用协议	请选择应用协议 多选
服务	ftp 多选
时间段	all
动作	限流 *
描述	
整体限流Class	class2 *

配置从 trust 区域和 untrust 区域到 DMZ 区域 FTP 服务器的下载带宽限制引用 class3。

防火墙 > 限流策略 > 整体限流

整体限流 | 整体限流Class

修改整体限流策略

字段	值
源安全区域	dmz *
目的安全区域	trust *
源地址	10.10.10.0\0.0.0.255 （多选）
目的地址	any （多选）
用户	any （多选）
应用协议	请选择应用协议 （多选）
服务	ftp （多选）
时间段	all
动作	限流 *
描述	
整体限流Class	class3 *

防火墙 > 限流策略 > 整体限流

整体限流 | 整体限流Class

修改整体限流策略

源安全区域	dmz *
目的安全区域	untrust *
源地址	10.10.10.0\0.0.0.255 多选
目的地址	any 多选
用户	any 多选
应用协议	请选择应用协议 多选
服务	ftp 多选
时间段	all
动作	限流 *
描述	
整体限流Class	class3 *

Setp 7 配置每 IP 限流，配置 PC 带宽限制。选择“**防火墙 > 限流策略 > 每 IP 限流**”，在“**每 IP 限流策略列表**”中，单击“**新建**”，依次输入或选择各项参数，配置完成后单击“**应用**”。

创建每 IP 限流 class。Class4 为 Trust 到 Untrust 的 Outbound 方向上上传带宽限制，class5 为 Trust 到 Untrust 的 inbound 方向上下载带宽限制。

防火墙 > 限流策略 > 每IP限流

每IP限流 | 每IP限流Class

修改每IP限流Class

名称	class4 *
保证带宽	<8-10000000>kbps
最大带宽	400 <8-10000000>kbps
最大连接数	<1-1000000>

应用 返回

防火墙 > 限流策略 > 每IP限流

每IP限流 | 每IP限流Class

修改每IP限流Class

名称	class5	*
保证带宽		<8-10000000>kbps
最大带宽	600	<8-10000000>kbps
最大连接数		<1-1000000>

应用 返回

在 Trust 到 Untrust 的 Outbound 方向上配置每 IP 限流策略 1，引用 car-class class4，限制上传最大带宽为 400kbps。

防火墙 > 限流策略 > 每IP限流

每IP限流 | 每IP限流Class

修改每IP限流策略

源安全区域	trust	*
目的安全区域	untrust	*
源地址	10.1.1.0\0.0.0.255	多选
目的地址	any	多选
用户	any	多选
应用协议	请选择应用协议	多选
服务	ftp	多选
时间段	all	
动作	限流	*
描述		
限流对象	● 源地址 ○ 目的地址	
每IP限流Class	class4	*

在 Trust 到 Untrust 的 inbound 方向上配置每 IP 限流策略 2，引用 car-class class5，限制 P2P 下载最大带宽为 600kbps。

防火墙 > 限流策略 > 每IP限流

每IP限流 | 每IP限流Class

修改每IP限流策略

源安全区域	untrust	*
目的安全区域	trust	*
源地址	any	多选
目的地址	10.1.1.0\0.0.0.255	多选
用户	any	多选
应用协议	P2P文件共享	多选
服务	ftp	多选
时间段	all	
动作	限流	*
描述		
限流对象	○ 源地址 ◉ 目的地址	
每IP限流Class	class5	*

验证结果

\# 查看 FTP 服务器 IP 地址表信息。

```
[USG] display traffic-policy statistic per-ip car
Current total node: 1
--------------------------------------------------------------------------------------------------
IP Address          Type                SrcVrf->DstVrf                    SrcZone->DstZone
PolicyID         Passed Packets/Passed bytes          Droped Packets/Droped bytes
----------------------------------------------------------------------------------------------------------
10.1.1.1            Src                 public->public                    trust->untrust            0
1/86
[USG] display traffic-policy statistic shared car
Current Total Node: 1
-------------------------------------------------------------------------------------------------------
SrcVrf->DstVrf                    SrcZone->DstZone          Policy ID          Passed Packets/Passed
Bytes          Droped Packets/Droped Bytes
----------------------------------------------------------------------------------------------------------------
```

```
public->public                untrust->trust           1
10620/86444                                 0/0
[USG] display traffic-policy statistic shared connection
Current Total Node: 2
--------------------------------------------------------------------------
      SrcVrf->DstVrf              SrcZone->DstZone       Policy ID      CurConn
--------------------------------------------------------------------------
      public->public              untrust->dmz             1              2
      public->public                trust->dmz             1              1
```

3.2 负载均衡实验

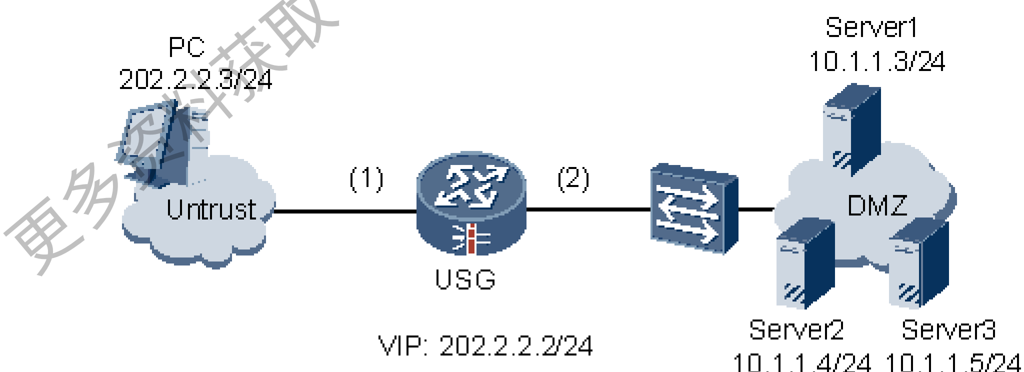
实验目的

内部网络中存在多个真实服务器对外提供 FTP 服务，配置负载均衡功能，保证流经 USG 的流量负载均衡。某内部网络中存在三台真实服务器对外提供 FTP 服务，IP 地址分别为 10.1.1.3/24、10.1.1.4/24 和 10.1.1.5/24，对外的虚拟 IP 地址为 202.2.2.2/24。要求配置 USG 的负载均衡功能，保证经过 USG 的流量负载均衡。

组网设备

PC 机一台，USG 系列防火墙一台，交换机一台，三台可作为服务器的 PC 机。

实验拓扑图



实验步骤(CLI)

Setp 1 配置 USG 基本功能。

配置 GigabitEthernet 0/0/1 的 IP 地址，并加入 Untrust 区域。

```
[USG] interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1] ip address 202.2.2.1 24
[USG-GigabitEthernet0/0/1] quit
```

```
[USG] firewall zone untrust
[USG-zone-untrust] add interface GigabitEthernet 0/0/1
[USG-zone-untrust] quit
```

配置 GigabitEthernet 0/0/2 的 IP 地址，并加入 DMZ 区域。

```
[USG] interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/2] ip address 10.1.1.1 24
[USG-GigabitEthernet0/0/2] quit
[USG] firewall zone dmz
[USG-zone-dmz] add interface GigabitEthernet 0/0/0
[USG-zone-dmz] quit
```

配置域间包过滤，以保证网络基本通信正常。

```
[USG] firewall packet-filter default permit interzone untrust dmz
[USG] firewall packet-filter default permit interzone local dmz
```

说明：

由于 USG 缺省对真实服务器进行健康检查，此时需要配置允许健康检查报文在 USG 的 Local 和 DMZ 域间出方向流动。

若需配置严格的域间包过滤，则需配置域间包过滤的源或者目的 IP 地址为真实服务器的 IP。

Setp 2 配置负载均衡功能。

启用负载均衡功能。

```
[USG] slb enable
[USG] slb
[USG-slb] rserver 1 rip 10.1.1.3 weight 32
[USG-slb] rserver 2 rip 10.1.1.4 weight 16
[USG-slb] rserver 3 rip 10.1.1.5 weight 32
```

配置真实服务器加入负载均衡组。

```
[USG-slb] group test
[USG-slb-group-test] metric srchash
[USG-slb-group-test] addrserver 1
[USG-slb-group-test] addrserver 2
[USG-slb-group-test] addrserver 3
[USG-slb-group-test] quit
```

配置虚服务器 IP 地址和端口号。

```
[USG-slb] vserver test vip 202.2.2.2 group test tcp
[USG-slb] quit
```

实验步骤(Web)

Setp 1 配置 USG 基本功能。

配置 GigabitEthernet 0/0/1 的 IP 地址，并加入 Untrust 区域。

网络 > 接口 > 接口

修改GigabitEthernet

接口名称	GigabitEthernet0/0/1 *	
别名		
VPN实例	public *	
安全区域	untrust	
模式	◉ 路由 ○ 交换	
连接类型	◉ 静态IP ○ DHCP ○ PPPoE	
IP地址	202 . 2 . 2 . 1	IP地址详细配置
子网掩码	255 . 255 . 255 . 0	
默认网关	. . .	

配置 GigabitEthernet 0/0/0 的 IP 地址，并加入 DMZ 区域。

网络 > 接口 > 接口

修改GigabitEthernet

接口名称	GigabitEthernet0/0/0 *	
别名		
VPN实例	public *	
安全区域	dmz	
模式	◉ 路由 ○ 交换	
连接类型	◉ 静态IP ○ DHCP ○ PPPoE	
IP地址	10 . 1 . 1 . 1	IP地址详细配置
子网掩码	255 . 255 . 255 . 0	
默认网关	. . .	

配置域间包过滤，以保证网络基本通信正常。

防火墙 > 安全策略 > 转发策略

修改转发策略

源安全区域	untrust *
目的安全区域	dmz *
源地址	any
目的地址	any
用户	请选择或输入用户或用户组
服务	请选择服务
时间段	all
动作	permit *

应用 返回

防火墙 > 安全策略 > 本地策略

修改对设备访问控制

源安全区域	dmz
源地址	any
服务	请选择服务
时间段	all
动作	permit

应用 返回

说明：

由于 USG 缺省对真实服务器进行健康检查，此时需要配置允许健康检查报文在 USG 的 Local 和 DMZ 域间出方向流动。

若需配置严格的域间包过滤，则需配置域间包过滤的源或者目的 IP 地址为真实服务器的 IP。

Setp 2 配置负载均衡功能。

\# 启用负载均衡功能。选择“**防火墙 > NAT > 负载均衡**”，选中“**负载均衡功能**”后面对应的“**启用**”复选框，单击“**应用**”。

防火墙 > NAT > 负载均衡

基本配置

负载均衡功能 ☑启用 应用

\# 配置真实服务器加入负载均衡组。选择“**防火墙 > NAT > 负载均衡**”，在“**负载均衡列表**”中，单击“**新建**”，依次输入或选择各项参数，单击“**应用**”。

防火墙 > NAT > 负载均衡

新建负载均衡

虚服务器名称 Test *
虚服务器IP 202 . 2 . 2 . 2 *
协议 any
算法 srchash
各个实服务器按照源地址分担流量，相同源地址的流量分配到固定的实服务器。
VRRP <1-255>

实服务器

新建 删除 刷新

	实服务器IP	权值 <1-63>	描述	连接控制
☑	10.1.1.5	32		自动检测
☐	10.1.1.4	16		自动检测
☐	10.1.1.3	32		自动检测

注意：虚服务器必须至少要包含一个实服务器。如果配置的实服务器已被其他虚拟服务器绑定，则该虚拟服务器IP必须与其他虚拟服务器IP一致，且协议和端口号不相同；否则，当该虚拟服务器IP与其他虚拟服务器IP冲突时，必须配置协议和端口号使之与其他虚服务器不相同或者更换IP。

应用 返回

验证结果

配置完成后，当 Untrust 区域的 PC 通过虚服务器 IP 地址 202.2.2.2/24 访问 DMZ 区域的 Server 时，可通过以下方式查看会话信息，存在三条到真实服务器的会话，说明 USG 对 FTP 服务器的流量实现了负载均衡。

```
<USG> display firewall session table
Current total sessions : 3
 ftp VPN:public --> public 202.2.2.3:3327-->202.2.2.2:21[10.1.1.4:21]
 ftp VPN:public --> public 202.2.2.3:3327-->202.2.2.2:21[10.1.1.5:21]
 ftp VPN:public --> public 202.2.2.3:3327-->202.2.2.2:21[10.1.1.6:21]
```

4 防火墙可靠性技术

4.1 BFD实验

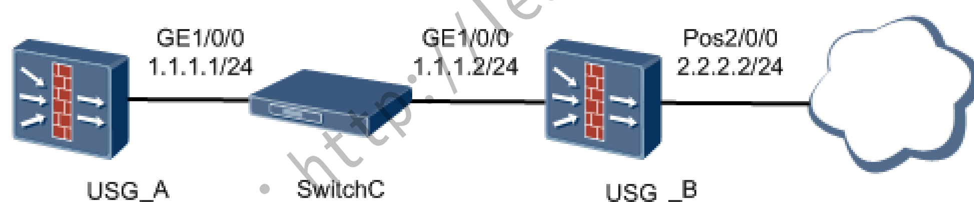
实验目的

通过配置静态路由绑定 BFD 检测链路是否发生故障。

组网设备

USG 防火墙 2 台，交换机一台。

实验拓扑图



实验步骤(命令行)

配置 USG_A。

Setp 1 配置各接口的 IP 地址（略）。

Setp 2 进入 Trust 区域视图，并将接口加入安全区域。

```
[USG_A] firewall zone trust
[USG_A-zone-trust] add interface GigabitEthernet1/0/0
[USG_A-zone-trust] quit
```

Setp 3 配置 Local 和 Trust 的域间安全策略。

```
[USG_A] policy interzone local trust outbound
[USG_A-policy-interzone-local-trust-outbound] policy 0
[USG_A-policy-interzone-local-trust-outbound-0] policy source any
[USG_A-policy-interzone-local-trust-outbound-0] action permit
[USG_A-policy-interzone-local-trust-outbound-0] quit
[USG_A] policy interzone local trust inbound
```

```
[USG_A-policy-interzone-local-trust-inbound] policy 0
[USG_A-policy-interzone-local-trust-inbound-0] policy source any
[USG_A-policy-interzone-local-trust-inbound-0] action permit
[USG_A-policy-interzone-local-trust-inbound-0] quit
```

Setp 4 在 USG_A 上配置与 USG_B 之间的 BFD Session。

```
[USG_A] bfd
[USG_A-bfd] quit
[USG_A] bfd aa bind peer-ip 1.1.1.2
[USG_A-bfd-session-aa] discriminator local 10
[USG_A-bfd-session-aa] discriminator remote 20
[USG_A-bfd-session-aa] commit
[USG_A-bfd-session-aa] quit
```

配置 USG_B。

Setp 5 进入 Trust 区域视图，并将接口加入安全区域。

```
[USG_B] firewall zone trust
[USG_B-zone-trust] add interface GigabitEthernet1/0/0
[USG_B-zone-trust] add interface POS2/0/0
[USG_B-zone-trust] quit
```

Setp 6 配置 Local 和 Trust 的域间安全策略。

```
[USG_B] policy interzone local trust outbound
[USG_B-policy-interzone-local-trust-outbound] policy 0
[USG_B-policy-interzone-local-trust-outbound-0] policy source any
[USG_B-policy-interzone-local-trust-outbound-0] action permit
[USG_B-policy-interzone-local-trust-outbound-0] quit
[USG_B] policy interzone local trust inbound
[USG_B-policy-interzone-local-trust-inbound] policy 0
[USG_B-policy-interzone-local-trust-inbound-0] policy source any
[USG_B-policy-interzone-local-trust-inbound-0] action permit
[USG_B-policy-interzone-local-trust-inbound-0] quit
```

Setp 7 在 USG_B 上配置与 USG_A 之间的 BFD Session。

```
[USG_B] bfd
[USG_B-bfd] quit
[USG_B] bfd bb bind peer-ip 1.1.1.1
[USG_B-bfd-session-bb] discriminator local 20
[USG_B-bfd-session-bb] discriminator remote 10
[USG_B-bfd-session-bb] commit
[USG_B-bfd-session-bb] quit
```

Setp 8 配置静态缺省路由并绑定 BFD 会话

在 USG_A 上配置到外部网络的静态缺省路由，并绑定 BFD 会话 aa。

```
[USG_A] ip route-static 0.0.0.0 0 1.1.1.2 track bfd-session aa
```

验证结果

配置完成后，在 USG_A 和 USG_B 上执行 **display session all** 命令，可以看到 BFD 会话已经建立，且状态为 Up。在系统视图下执行 **display current-configuration | include** 命令，可以看到静态路由已经绑定 BFD 会话。以 USG_A 上的显示为例。

```
[USG_A] display bfd session all
--------------------------------------------------------------------------------
Local   Remote PeerIpAddr        State      Type       InterfaceName
--------------------------------------------------------------------------------
10      20       1.1.1.2             Up                                  -
--------------------------------------------------------------------------------
        Total UP/DOWN Session Number : 1/0
[USG_A] display current-configuration | include bfd
 bfd
bfd aa bind peer-ip 1.1.1.2
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2 track bfd-session aa
```

在 USG_A 上查看 IP 路由表，静态路由存在于路由表中。

```
[USG_A] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
             Destinations : 3            Routes : 3
Destination/Mask     Proto   Pre   Cost        Flags NextHop            Interface
            0.0.0.0/0     Static 60     0            RD    1.1.1.2
GigabitEthernet1/0/0
            1.1.1.0/24    Direct 0      0              D    1.1.1.1
GigabitEthernet1/0/0
            1.1.1.1/32    Direct 0      0              D    127.0.0.1
InLoopBack0
```

对 USG_B 的接口 GE1/0/0 执行 shutdown 命令模拟链路故障。

```
[USG_B] interface GigabitEthernet 1/0/0
[USG_B-GigabitEthernet1/0/0] shutdown
```

查看 USG_A 的路由表，发现静态缺省路由 0.0.0.0/0 也不存在了。因为静态缺省路由绑定了 BFD 会话，当 BFD 检测到故障后，就会迅速通知所绑定的静态路由不可用。

```
[USG_A] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
             Destinations : 1            Routes : 1
```

```
Destination/Mask        Proto   Pre   Cost        Flags NextHop          Interface
            1.1.1.1/32  Direct 0      0               D   127.0.0.1
InLoopBack0
```

4.2 Eth-Trunk实验

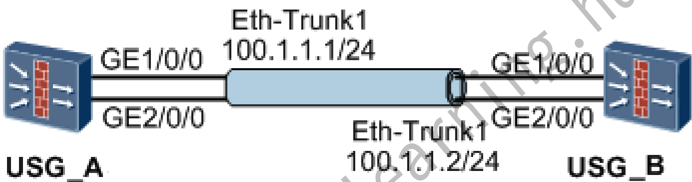
实验目的

配置三层手工负载分担模式 Eth-Trunk 接口，该组网的特点是 Eth-Trunk 的建立，成员接口的加入，以及哪些接口作为活动接口完全由手工来配置，没有链路聚合控制协议的参与。该模式下所有活动接口都参与数据的转发，分担负载流量。

组网设备

USG 系列防火墙 2 台。

实验拓扑图



实验步骤(命令行)

配置 USG_A

Setp 1 创建 Eth-Trunk 接口，并配置 IP 地址。

```
[USG_A] interface eth-trunk 1
[USG_A-Eth-Trunk1] ip address 100.1.1.1 255.255.255.0
[USG_A-Eth-Trunk1] quit
```

Setp 2 将接口 GE1/0/0、GE2/0/0 加入到 Eth-Trunk 1 中。

```
[USG_A] interface gigabitethernet 1/0/0
[USG_A-GigabitEthernet1/0/0] undo shutdown
[USG_A-GigabitEthernet1/0/0] eth-trunk 1
[USG_A-GigabitEthernet1/0/0] quit
[USG_A] interface gigabitethernet 2/0/0
[USG_A-GigabitEthernet2/0/0] undo shutdown
[USG_A-GigabitEthernet2/0/0] eth-trunk 1
[USG_A-GigabitEthernet2/0/0] quit
```

Setp 3 配置 Eth-Trunk 1 加入 Trust 安全区域。

```
[USG_A] firewall zone trust
[USG_A-zone-trust] add interface eth-trunk 1
[USG_A-zone-trust] quit
```

Setp 4 配置域间安全策略。

[USG_A] **policy interzone local trust outbound**
[USG_A-policy-interzone-local-trust-outbound] **policy 0**
[USG_A-policy-interzone-local-trust-outbound-0] **policy source any**
[USG_A-policy-interzone-local-trust-outbound-0] **action permit**
[USG_A-policy-interzone-local-trust-outbound-0] **quit**
[USG_A-policy-interzone-local-trust-outbound] **quit**
[USG_A] **policy interzone local trust inbound**
[USG_A-policy-interzone-local-trust-inbound] **policy 0**
[USG_A-policy-interzone-local-trust-inbound-0] **policy source any**
[USG_A-policy-interzone-local-trust-inbound-0] **action permit**
[USG_A-policy-interzone-local-trust-inbound-0] **quit**
[USG_A-policy-interzone-local-trust-inbound] **quit**

配置 USG_B

Setp 5 创建 Eth-Trunk 接口，并配置 IP 地址。

[USG_B] **interface eth-trunk 1**
[USG_B-Eth-Trunk1] **ip address 100.1.1.2 255.255.255.0**
[USG_B-Eth-Trunk1] **quit**

Setp 6 将接口 GE1/0/0、GE2/0/0 加入到 Eth-Trunk 1 中。

[USG_B] **interface gigabitethernet 1/0/0**
[USG_B-GigabitEthernet1/0/0] **undo shutdown**
[USG_B-GigabitEthernet1/0/0] **eth-trunk 1**
[USG_B-GigabitEthernet1/0/0] **quit**
[USG_B] **interface gigabitethernet 2/0/0**
[USG_B-GigabitEthernet2/0/0] **undo shutdown**
[USG_B-GigabitEthernet2/0/0] **eth-trunk 1**
[USG_B-GigabitEthernet2/0/0] **quit**

Setp 7 配置 Eth-Trunk 1 加入 Trust 安全区域。

[USG_B] **firewall zone trust**
[USG_B-zone-trust] **add interface eth-trunk 1**
[USG_B-zone-trust] **quit**

Setp 8 配置域间安全策略。

[USG_B] **policy interzone local trust outbound**
[USG_B-policy-interzone-local-trust-outbound] **policy 0**
[USG_B-policy-interzone-local-trust-outbound-0] **policy source any**
[USG_B-policy-interzone-local-trust-outbound-0] **action permit**
[USG_B-policy-interzone-local-trust-outbound-0] **quit**
[USG_B-policy-interzone-local-trust-outbound] **quit**
[USG_B] **policy interzone local trust inbound**
[USG_B-policy-interzone-local-trust-inbound] **policy 0**
[USG_B-policy-interzone-local-trust-inbound-0] **policy source any**

[USG_B-policy-interzone-local-trust-inbound-0] **action permit**
[USG_B-policy-interzone-local-trust-inbound-0] **quit**
[USG_B-policy-interzone-local-trust-inbound] **quit**

验证结果

在 USG_A 或 USG_B 上执行 **display interface eth-trunk** 命令，可以看到接口状态为 UP。以 USG_A 的显示为例。

```
[USG_A] display interface eth-trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-08-10 03:57:08 UTC+08:00
Description: Eth-Trunk1 Interface
Route Port,Hash arithmetic : According to flow,Maximal BW: 2G, Current BW: 2G,
T
he Maximum Transmit Unit is 1500
Internet Address is 100.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
0018-8249-2a8d
Physical is ETH_TRUNK
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 packets,0 bytes,
           0 unicast,0 broadcast,0 multicast
           0 errors,0 drops,
    Output:1 packets,64 bytes,
           0 unicast,1 broadcast,0 multicast
           0 errors,0 drops
    Input bandwidth utilization    : 0.00%
    Output bandwidth utilization : 0.01%
-----------------------------------------------------
PortName                     Status                  Weight
-----------------------------------------------------
GigabitEthernet1/0/0       UP                      1
GigabitEthernet2/0/0       UP                      1
-----------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

USG_A 和 USG_B 的 Eth-Trunk 接口能够互相 Ping 通。

```
[USG_A] ping -a 100.1.1.1 100.1.1.2
```

```
PING 100.1.1.2: 56   data bytes, press CTRL_C to break
    Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=31 ms
    Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=31 ms
    Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=62 ms
    Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=62 ms
    Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=62 ms
--- 100.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 31/49/62 ms
```

4.3 IP-Link 实验

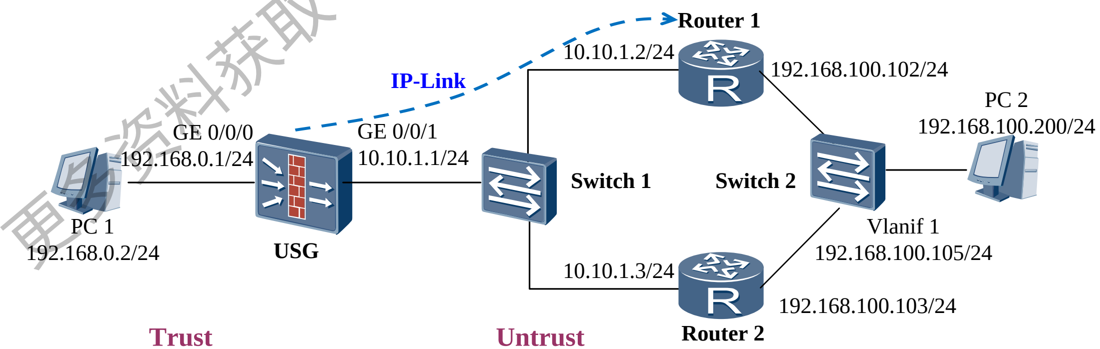
实验目的

配置静态路由与 IP-Link 联动。某公司通过交换机连接两个路由器，以双链路接入 Internet，为了保证在链路故障时可以动态调整静态路由，在 USG 和两台路由器之间配置静态路由绑定 IP-Link，将 Router 1 作为主要使用的路由器，在出现故障时，动态启用到 Router 2 的路由，从而不影响内网用户正常访问 Internet。

组网设备

PC 机两台、USG 系列防火墙一台、交换机两台，路由器两台。

实验拓扑图



实验步骤(命令行)

Setp 1 配置各接口的 IP 地址。并将接口加入安全区域，配置域间包过滤，以保证网络基本通信正常。

```
<USG> system-view
[USG] interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0] ip address 192.168.0.1 255.255.255.0
```

```
[USG-GigabitEthernet0/0/0] quit
[USG] interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1] ip address 10.10.1.1 255.255.255.0
[USG-GigabitEthernet0/0/1] quit
[USG]firewall zone untrust
[USG-zone-untrust]add interface GigabitEthernet 0/0/1
[USG]firewall packet-filter default permit interzone untrust trust
```

Setp 2 配置 NAT 策略。使内网 PC 可以与外网 PC 通信。

```
[USG]nat-policy interzone trust untrust outbound
[USG-nat-policy-interzone-trust-untrust-outbound]policy 0
[USG-nat-policy-interzone-trust-untrust-outbound-0]action source-nat
[USG-nat-policy-interzone-trust-untrust-outbound-0]easy-ip GigabitEthernet 0/0/1
```

Setp 3 配置 IP-Link，分别检测 USG 到 Router 1 和 Router 2 的链路。

```
[USG] ip-link check enable
[USG] ip-link 1 destination 10.10.1.2 mode icmp
[USG] ip-link 2 destination 10.10.1.3 mode icmp
```

Setp 4 配置到 Internet 静态路由，分别绑定各自链路的 IP-Link，为通过 Router 1 的路由设置较高的优先级。

```
[USG] ip route-static 0.0.0.0 0.0.0.0 10.10.1.2 track ip-link 1
[USG] ip route-static 0.0.0.0 0.0.0.0 10.10.1.3 preference 70 track ip-link 2
```

Setp 5 配置交换机。

Switch 1 为透传模式，可不做任何配置。

Switch 2 上将三个接口加入同一 vlan，并配置 vlanif 接口。PC2 的网关地址为该 vlanif 接口地址。

```
[SW2] interface Vlanif 1
[SW2-Vlanif1] ip address 192.168.100.105 24
```

在 switch 2 上配置动态路由协议 OSPF。通告 192.168.100.0/24 网段。

```
[SW2] ospf 100
[SW2-ospf-100] area 0
[SW2-ospf-100-area-0.0.0.0] network 192.168.100.0 0.0.0.255
```

Setp 6 配置路由器。

配置各路由器接口 IP 地址。具体步骤省略。

在 Router 1 和 Router 2 上分别配置 OSPF，通告 10.10.1.0/24 网段和 192.168.100.0/24 网段路由。以 Router 1 配置为例。Router 2 配置类似，具体步骤省略。

```
[Router 1] ospf 100
[Router 1-ospf-100]area 0
[Router 1-ospf-100-area-0.0.0.0]network 10.10.1.0 0.0.0.255
[Router A-ospf-100-area-0.0.0.0]network 192.168.100.0 0.0.0.255
```

实验步骤(Web)

Setp 1 配置各接口的 IP 地址。并将接口加入安全区域。具体步骤省略。

Setp 2 配置域间包过滤策略，使网络正常通信。

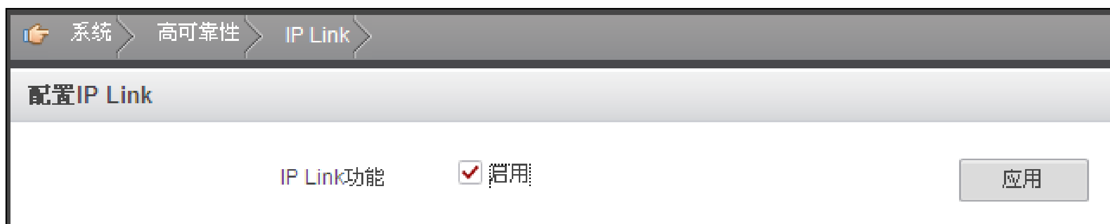


Setp 3 配置 NAT 策略。使内网 PC 可以与外网 PC 通信。



Setp 4 配置 IP-Link，分别检测 USG 到 Router 1 和 Router 2 的链路。

\# 选择“**系统 > 高可靠性 > IP Link**”，选中“**IP Link 功能**”对应的“**启用**”，启用 IP-Link 功能。



\# 在“**IP Link 列表**”中，单击“**新建**”，新建 IP-link。选择待侦测目的配置方式为 IP 地址，分别检测到达 10.10.1.2 和 10.10.1.3 地址的 IP-link。

系统 > 高可靠性 > IP Link

新建IP Link

IP Link号 1 *<1-128>
待侦测目的IP配置方式 IP地址 域名
IP地址 10 . 10 . 1 . 2 *
绑定出接口 ----- NONE -----
监控组 ----- NONE -----
超时时间 3 *<1-100>秒
探测模式 ICMP ARP

应用 返回

系统 > 高可靠性 > IP Link

新建IP Link

IP Link号 2 *<1-128>
待侦测目的IP配置方式 IP地址 域名
IP地址 10 . 10 . 1 . 3 *
绑定出接口 ----- NONE -----
监控组 ----- NONE -----
超时时间 3 *<1-100>秒
探测模式 ICMP ARP

应用 返回

Setp 5 配置到 Internet 静态路由。选择“**路由 > 静态 > 静态路由**”，在“**静态路由列表**”中，单击“**新建**”依次输入或选择各项参数，在“**IP Link 号**”一栏中分别绑定各自链路的 IP-Link，为通过 Router 1 的路由设置较高的优先级。

路由 > 静态 > 静态路由

新建静态路由

目的地址	0 . 0 . 0 . 0 *
掩码	0 . 0 . 0 . 0 *
下一跳	10 . 10 . 1 . 2 下一跳和接口不能同时为空
接口	----- NONE -----
IP Link号	1
优先级	60 <1-255>

应用 返回

路由 > 静态 > 静态路由

新建静态路由

目的地址	0 . 0 . 0 . 0 *
掩码	0 . 0 . 0 . 0 *
下一跳	10 . 10 . 1 . 3 下一跳和接口不能同时为空
接口	----- NONE -----
IP Link号	2
优先级	70 <1-255>

应用 返回

Setp 6 配置交换机。

Switch 1 为透传模式，可不做任何配置。

Switch 2 上将三个接口加入同一 vlan，并配置 vlanif 接口。PC2 的网关地址为该 vlanif 接口地址。

[SW2]**interface Vlanif 1**

[SW2-Vlanif1]**ip address 192.168.100.105 24**

在 switch 2 上配置动态路由协议 OSPF。通告 192.168.100.0/24 网段。

[SW2]**ospf 100**

[SW2-ospf-100]**area 0**

[SW2-ospf-100-area-0.0.0.0]**network 192.168.100.0 0.0.0.255**

Setp 7 配置路由器。

配置各路由器接口 IP 地址。具体步骤省略。

在 Router 1 和 Router 2 上分别配置 OSPF，通告 10.10.1.0/24 网段和 192.168.100.0/24 网段路由。以 Router 1 配置为例。Router 2 配置类似，具体步骤省略。

[Router 1] **ospf 100**

[Router 1-ospf-100]**area 0**

[Router 1-ospf-100-area-0.0.0.0]**network 10.10.1.0 0.0.0.255**

[Router A-ospf-100-area-0.0.0.0]**network 192.168.100.0 0.0.0.255**

验证结果

在 10.10.1.2 链路工作正常时，从 PC1 tracert 到 PC2，获得如下结果：

```
C:\Documents and Settings\Administrator>tracert 192.168.100.200

Tracing route to 192.168.100.200 over a maximum of 30 hops

  1     *        *        *     Request timed out.
  2     2 ms     2 ms     2 ms  10.10.1.2
  3    <1 ms    <1 ms    <1 ms  192.168.100.200

Trace complete.
```

在 PC1 上运行 ping 192.168.100.200 –t 命令。然后在 Router1 上将 10.10.1.2 接口 shutdown。将会出现如下结果，当 router 1 接口 down 掉时，IP-link 将会采用 router2 的链路继续与 PC2 通信。

```
C:\Documents and Settings\Administrator>ping 192.168.100.200 -t

Pinging 192.168.100.200 with 32 bytes of data:

Reply from 192.168.100.200: bytes=32 time<1ms TTL=125
Reply from 192.168.100.200: bytes=32 time<1ms TTL=125
Reply from 192.168.100.200: bytes=32 time<1ms TTL=125
Reply from 192.168.100.200: bytes=32 time<1ms TTL=125
Request timed out.
Reply from 192.168.100.200: bytes=32 time<1ms TTL=125
Reply from 192.168.100.200: bytes=32 time<1ms TTL=125
Reply from 192.168.100.200: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.100.200:
    Packets: Sent = 18, Received = 17, Lost = 1 (5% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

在 Router1 上将 10.10.1.2 接口 shutdown 后，在 PC1 上再次 tracert 192.168.100.200，将会出现如下结果：

```
C:\Documents and Settings\Administrator>tracert 192.168.100.200

Tracing route to 192.168.100.200 over a maximum of 30 hops

  1     *        *        *     Request timed out.
  2     2 ms     2 ms     2 ms  10.10.1.3
  3    <1 ms    <1 ms    <1 ms  192.168.100.200
```

```
Trace complete.
```

可以看到，此时，防火墙已经选择 router2 的 10.10.1.3 接口进行数据包转发。

4.4 防火墙双机热备实验（主备备份）

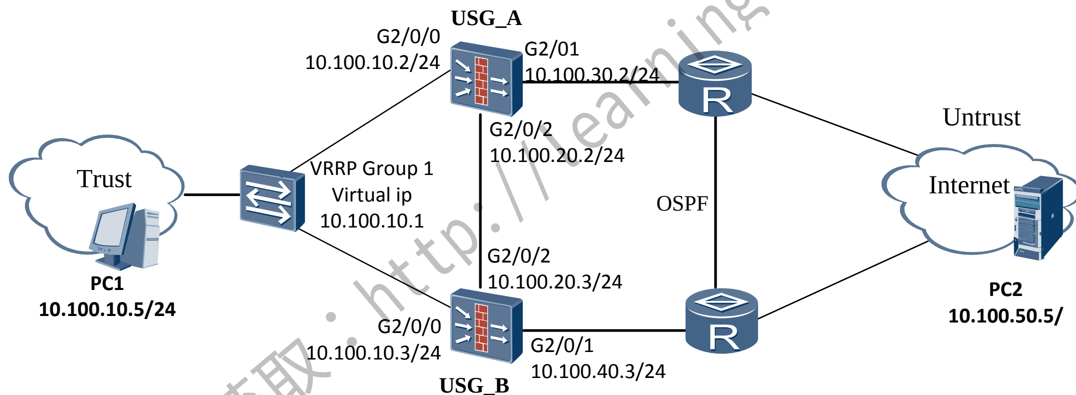
实验目的

完成双机热备和 OSPF 的结合使用的配置并理解其实现原理，两台 USG 防火墙和路由器之间运行动态路由 OSPF 协议，和交换机之间运行 VRRP 协议。USG 的双机热备份功能基于 VRRP 实现，在 USG 的业务接口上配置一个 VRRP 备份组加入 VGMP 管理组的 Master 或 Slave 管理组，组成主备备份的组网。

组网设备

两台 PC 机，两台防火墙，两台交换机，两台路由器。

实验拓扑图



路由器侧 IP 地址可根据防火墙侧地址网段自行规划，且使用 OSPF 学习路由信息。

实验步骤(CLI)

配置 USG_A。

Setp 1 配置各接口 IP 地址，并加入相应安全区域。

```
<USG> system-view
[USG] interface GigabitEthernet 2/0/0
[USG-GigabitEthernet2/0/0] ip address 10.100.10.2 24
[USG-GigabitEthernet2/0/0] quit
[USG] firewall zone trust
[USG-zone-trust] add interface GigabitEthernet 2/0/0
[USG-zone-trust] quit
```

```
[USG] interface GigabitEthernet 2/0/1
[USG-GigabitEthernet2/0/1] ip address 10.100.30.2 24
[USG-GigabitEthernet2/0/1] quit
[USG] firewall zone untrust
[USG-zone-untrust] add interface GigabitEthernet 2/0/1
[USG-zone-untrust] quit
[USG] interface GigabitEthernet 2/0/2
[USG-GigabitEthernet2/0/2] ip address 10.100.20.2 24
[USG-GigabitEthernet2/0/2] quit
[USG] firewall zone dmz
[USG-zone-dmz] add interface GigabitEthernet 2/0/2
[USG-zone-dmz] quit
```

Setp 2 在接口 GigabitEthernet 2/0/0 上配置 VRRP 备份组 1，并配置备份组的虚拟 IP 地址。

```
[USG] interface GigabitEthernet 2/0/0
[USG-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.100.10.1 master
[USG-GigabitEthernet2/0/0] quit
```

Setp 3 在 USG A 上配置运行 OSPF 动态路由协议。

```
[USG] ospf 101
[USG-ospf-101] area 0
[USG-ospf-101-area-0.0.0.0] network 10.100.30.0 0.0.0.255
[USG-ospf-101-area-0.0.0.0] quit
```

NOTE：

配置 OSPF 动态路由协议的时候，请打开 Untrust 域和 Local 域的域间包过滤，避免阻塞正常的路由协议报文。USG A 运行 OSPF 协议对外发布路由时，不能发布与交换机相连的网段的路由。

Setp 4 在 USG A 上配置引入与交换机相连的网段的直连路由。

```
[USG] acl 2009
[USG-acl-basic-2009] description forRoutePolicyOnly
[USG-acl-basic-2009] rule permit source 10.100.10.0 0.0.255.255
[USG-acl-basic-2009] quit
[USG] route-policy r1 permit node 1
[USG-route-policy] if-match acl 2009
[USG-route-policy] quit
[USG] ospf 101
[USG-ospf-101] import-route direct route-policy r1
[USG-ospf-101] quit
```

NOTE：

引入直连路由时，不能引入 HRP 备份通道接口所在网段的路由。因此必须通过配置路由策略只引入与交换机相连的网段的直连路由。

Setp 5 配置根据 HRP 状态调整 OSPF 的相关 COST 值的功能。

```
[USG] hrp ospf-cost adjust-enable
```

NOTE：

USG 工作在路由模式下且部署于 OSPF 网络中做双机热备份时，主备 USG 上都必须配置该命令。

Setp 6 配置 VGMP 管理组的抢占功能为开启状态，且抢占延迟大于故障恢复后 OSPF 协议的收敛时间。

```
[USG] hrp preempt delay 60
```

NOTE：

根据实际组网情况分析故障恢复后 OSPF 协议的收敛时间，必须配置此抢占延迟大于 OSPF 的收敛时间。

Setp 7 在接口视图下配置 Master 管理组监视接口状态。

```
[USG] interface GigabitEthernet 2/0/1
[USG-GigabitEthernet2/0/1] hrp track master
[USG-GigabitEthernet2/0/1] quit
```

Setp 8 配置会话快速备份。

```
[USG] hrp mirror session enable
```

\# 配置 HRP 备份通道。

```
[USG] hrp interface GigabitEthernet 2/0/2
```

NOTE：

主备 USG 的 HRP 备份通道接口必须直接相连，中间不能连接交换机

Setp 9 启动 HRP。

```
[USG] hrp enable
```

配置 USG B

USG B 和 USG A 的配置基本相同，不同之处在于：

1) USG B 各接口的 IP 地址与 USG A 各接口的 IP 地址不相同。
2) 在 USG B 的接口 GigabitEthernet 2/0/0 上配置 VRRP 备份组时，与 USG A 的 Master 管理组对应的必须配置为 Slave 管理组。
3) 在 USG B 上不需要配置 VGMP 管理组的抢占功能。

在 USG A 上启动配置命令的自动备份、配置 ACL，并配置 Trust 区域和 Untrust 区域的域间包过滤规则。

Setp 10 启动配置命令的自动备份功能。

```
HRP_M[USG] hrp auto-sync config
```

Setp 11 创建基本 ACL 2000，配置源地址为 10.100.10.0/24 的规则。

```
HRP_M[USG] acl 2000
HRP_M[USG-acl-basic-2000] rule permit source 10.100.10.0 0.0.0.255
HRP_M[USG-acl-basic-2000] quit
```

Setp 12 配置 Trust 区域和 Untrust 区域的域间包过滤规则。

```
HRP_M[USG] firewall interzone trust untrust
HRP_M[USG-interzone-trust-untrust] packet-filter 2000 outbound
```

```
HRP_M[USG-interzone-trust-untrust] quit
```

配置路由器。

Setp 13 在路由器上配置 OSPF，命令较为简单，以其中一台为例介绍配置命令，另外一台类似

```
[Router A] ospf 101
[Router A-ospf-101]area 0
[Router A-ospf-101-area-0.0.0.0]network 10.100.30.0 0.0.0.255
[Router A-ospf-101-area-0.0.0.0]network 192.168.1.0 0.0.0.255(与另外一台路由器互连网段位 192.168.1.0/24)
```

配置交换机。

实际应用中，Switch 与 USG 相连的接口一般是二层接口，配置 USGA、USG B 连接到 Switch 的接口以及 Switch 连接到 Trust 区域的接口，将此三个接口加入同一个 VLAN 2,在 PC1 上配置静态路由，将 VRRP 备份组 2 的虚拟 IP 地址作为到达其他网段的下一跳地址，以其中一台交换机接口配置为例，其他接口类似。

```
[Switch A]vlan 2
[Switch A-GigabitEthernet0/0/1]port link-type access
[Switch A-GigabitEthernet0/0/1]port default vlan 2
```

实验步骤(Web)

配置 USG A。

Setp 1 选择“**网络 > 接口**”，显示“**接口**”界面。 单击各接口对应的 ，显示“**配置 GigabitEthernet**”界面。按照拓扑图配置各接口 IP 地址并将其加入各安全区域。具体步骤省略。配置完成后，单击“**应用**”。

Setp 2 配置 USG A 的 VRRP 备份组。 选择“**系统 > 高可靠性**”。 选择“**双机热备**”页签。在“**VRID 列表**”界面，单击 新建，显示“**新建 VRID**”界面。配置 VRRP 备份组 1，参数配置如下图所示。

系统 > 高可靠性 > 双机热备

新建VRID

VRRP VRID: 1 *<1-255>
接口名称: GE2/0/0 * 查看配置
接口IP地址/掩码: 10.100.10.2 * 255.255.255.0
虚IP地址/掩码: 10.100.10.1 * 255.255.255.0
管理组: Active / Standby
高级
应用 返回

Setp 3 配置 USG A 上运行 OSPF 动态路由协议。选择“**路由 > 动态路由**”。选择“**OSPF**”页签，单击新建，显示“**新建 OSPF**”界面。配置 OSPF，参数配置如下图所示。

路由 > 动态 > OSPF

新建OSPF

进程ID: 101 *<1-65535>
路由器ID: 10.100.10.2
SPF计算间隔: 5 秒
内部优先级: 10 <1-255>
ASE优先级: 150 <1-255>
通告缺省路由
应用 返回

Setp 4 在 OSPF 进程 101 的右侧，单击，在“**区域配置**”栏中，单击新建，显示“**新建区域**”界面。在区域 0 里面发布 10.100.30.0/24 网络路由，参数配置如下图所示。

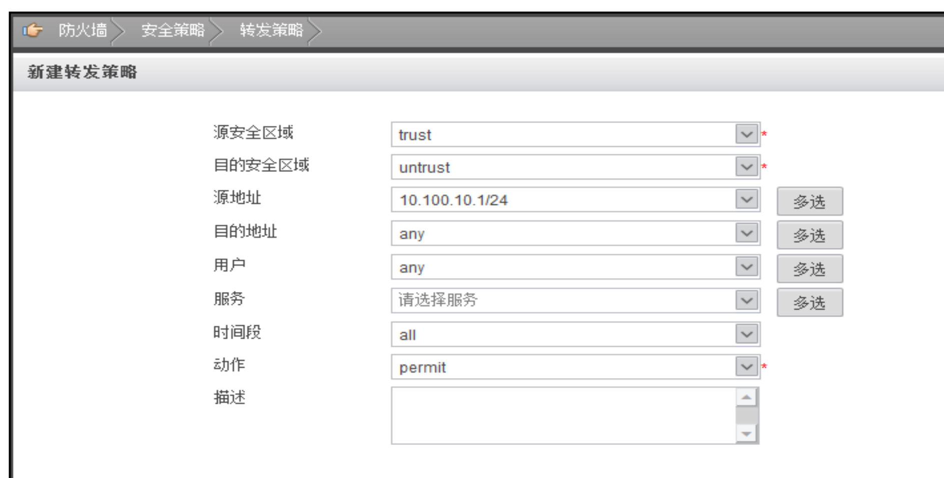
单击“**应用**”。

Setp 5 启动 USG A 的 HRP 功能。选择“**系统 > 可靠性**”。选择“**双机热备**”页签。在“**双机热备**”界面，选中“**HRP 启动**”前的复选框，选择 GigabitEthernet 2/0/2 作为“**HRP 备份通道**”，如下图所示。

单击“**应用**”。

Setp 6 配置 USG A 的 HRP 状态监控组。在“**HRP 启动**”的“**高级**”栏中，单击“**配置 HRP 状态监控组**”右侧的“**配置**”，显示“**配置状态监控组**”界面。在 ，选择“**Interface**”，依次填入各参数，单击 添加 。配置完成后的显示应如下图所示。

Setp 7 在 USG A 上启动配置 ACL，并配置 Trust 区域和 Untrust 区域的域间包过滤规则。选择“**防火墙 > 转发策略**”点击 新建 ，配置参数如下。



配置 USG B。

USG B 和 USG A 的配置基本相同，不同之处在于：

1) USG B 各接口的 IP 地址与 USG A 各接口的 IP 地址不相同。
2) USG B 的 VRRP 指定的管理组应该设为 Slave。
3) USG B 的 GigabitEthernet 2/0/1 接口下的 HRP 状态监控组应该设为 Slave。

配置路由器。

在路由器上配置 OSPF，具体配置命令请参考路由器的相关文档。

配置 Switch。

实际应用中，Switch 与 USG 相连的接口一般是二层接口，配置 Switch 与 USG A、USG B 以及 Trust 或 Untrust 区域的设备相连的接口，并将此三个接口加入同一个 VLAN。

配置静态路由，将 VRRP 备份组的虚拟 IP 地址作为到达其他网段的下一跳地址。具体配置请参考交换机的相关文档。

验证结果

在 USG A 上执行 **display vrrp** 命令，检查 VRRP 备份组内接口的状态信息，显示以下信息表示 VRRP 备份组建立成功。

```
HRP_M[USG] display vrrp
  GigabitEthernet2/0/0 | Virtual Router 1
    VRRP Group : Master
    state : Master
    Virtual IP : 10.100.10.1
    Virtual MAC : 0000-5e00-0101
    Primary IP : 10.100.10.2
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
```

```
    Preempt : YES     Delay Time : 0
    Timer : 1
    Auth Type : NONE
    Check TTL : YES
```

在 USG A 上执行 display hrp state 命令，检查当前 HRP 的状态，显示以下信息表示 HRP 建立成功。

```
HRP_M[USG] display hrp state
 The firewall's config state is: MASTER

 Current state of virtual routers configured as master:
              GigabitEthernet2/0/0      vrid      1 : master
 Current state of interfaces tracked by master:
              GigabitEthernet2/0/1 : up
```

PC2 作为 HTTP 服务器位于 Untrust 区域，对外提供 HTTP 服务。在 Trust 区域的 PC1 端访问 Untrust 区域的 HTTP 服务器，并进行文件的下载操作。分别在 USG A 和 USG B 上检查会话。

```
HRP_M[USG] display firewall session table verbose
14:12:27  2010/02/01
 Current total sessions: 1
 http: VPN: public --> public
 Zone: trust --> untrust Slot: 4 CPU: 0 TTL: 00:00:10 Left: 00:00:03
 Interface: GigabitEthernet1/0/1 NextHop: 202.38.10.1
 <--packets: 908 bytes: 7548 -->packets: 23 bytes: 306
 acl: 2000   rule: 0
 10.100.10.3:2048 --> 202.38.10.1:80
HRP_S[USG_B] display firewall session table verbose
14:12:27  2010/02/01
 Current total sessions: 1
 http: VPN: public --> public
 Zone: trust --> untrust Remote Slot: 4 CPU: 0 TTL: 00:00:10 Left: 00:00:03
 Interface: GigabitEthernet1/0/1 NextHop: 202.38.10.1
 <--packets: 0 bytes: 0 -->packets: 0 bytes: 0
 acl: 2000   rule: 0
 10.100.10.3:2048 --> 202.38.10.1:80
```

分别在 USG A 和 USG B 上进行以下操作，检查 HRP 状态和 VRRP 备份组内接口的状态信息。

a) 选择“系统 > 可靠性”。

b) 选择“双机热备”页签。USG A、USG B 的显示信息分别如下图所示。

USG A 的主备状态



VRID列表

新建 删除 刷新

VRID	虚IP地址	所属备份组	状态
GigabitEthernet2/0/0 (备份通道: NO)			
1	10.100.10.1	Active	Master

第 1 页共 1 页

USG B 的主备状态

配置双机热备

HRP启动 HRP状态: Active 主组状态: Active 备组状态: Initialize

HRP备份通道 GigabitEthernet2/0/2 *对端IP地址 状态: running

高级

应用 刷新

VRID列表

新建 删除 刷新

VRID	虚IP地址	所属备份组	状态
GigabitEthernet2/0/0 (备份通道: NO)			
1	10.100.10.1	Slave	Backup

第 1 页共 1 页

在处于 Trust 区域的 PC1 端 ping 处于 Untrust 区域的 PC2 端，分别在 USG A 和 USG B 上进行以下操作，检查会话表。

a) 选择“系统 > 信息”。

b) 选择“会话表”页签，查看会话表项信息。

USG A 和 USG B 上都有对应的会话表项，表示配置双机热备份功能后，会话备份成功。

4.5 Link-group 实验

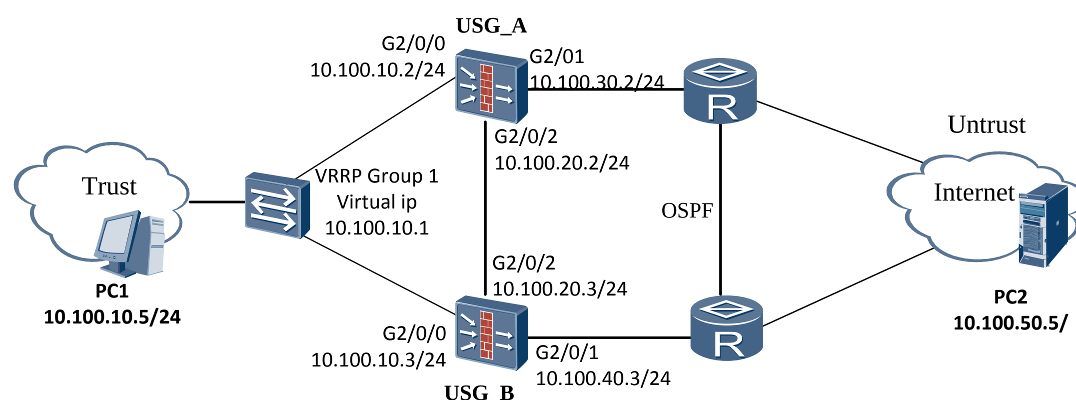
实验目的

在不进行 ip-link（链路检测）的情况下，当 FW 上行接口 down，VRRP 可以进行主备切换。在 4.4 防火墙双机热备实验的基础上完成该实验。

组网设备

两台 PC 机，两台防火墙，两台交换机，两台路由器。

实验拓扑图



实验步骤(命令行)

Setp 1 保持原 4.4 的实验环境与配置不变。

Setp 2 配置防火墙 A 接口 GigabitEthernet 2/0/0 加入到 Link-group 1

[USG_A] **interface GigabitEthernet 2/0/0**

[USG_A-GigabitEthernet2/0/0] **link-group 1**

[USG_A-GigabitEthernet2/0/0] **quit**

Setp 3 配置防火墙 A 接口 GigabitEthernet 2/0/1 加入到 Link-group 1

[USG_A] **interface GigabitEthernet 2/0/1**

[USG_A-GigabitEthernet2/0/1] **link-group 1**

[USG_A-GigabitEthernet2/0/1] **quit**

实验步骤(Web)

Setp 1 将防火墙 A 的各业务接口加入 link group 1 中。选择"**系统 > 高可靠性 > Link Group**"。在"**Link Group**"中，选择要配置的 Link Group，单击，在"**可选**"区域框中，选中 GE2/0/0 和 GE2/0/1 后单击 。



验证结果

当防火墙 A 接口 GE1/0/0 断掉时，观察主机热备切换速度及接口 GE2/0/1 的物理状态。

5 虚拟防火墙技术

5.1 虚拟防火墙实验

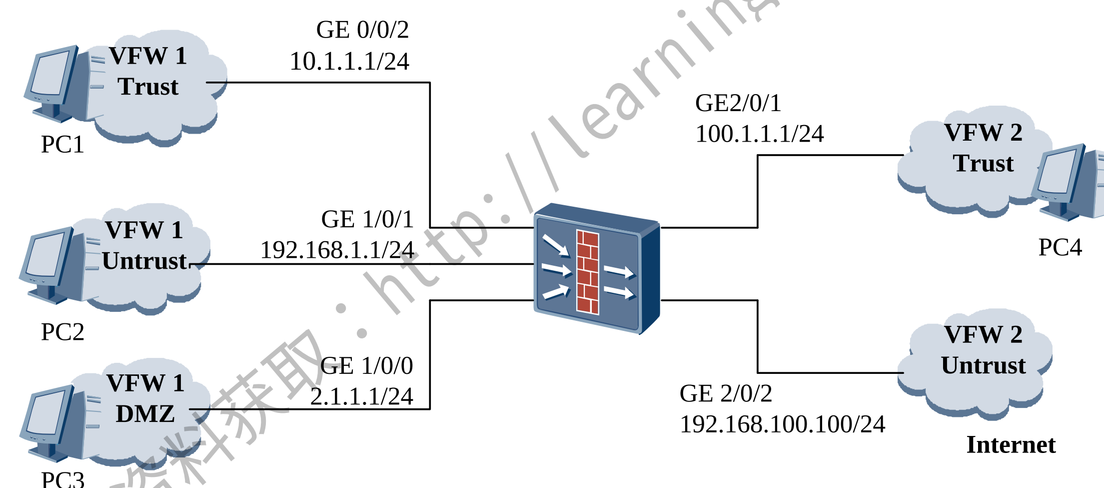
实验目的

掌握虚拟防火墙的典型组网并实现配置管理。

组网设备

PC 主机 6 台、USG 系列防火墙 1 台。

实验拓扑图



USG 统一安全网关向外提供出租业务，VPN 实例 vfw1 租给企业 A，vfw2 租给企业 B。

1 企业 A 和企业 B 能够地址重叠。

2 Vfw1 划分为 Trust、DMZ（Demilitarized Zone）、Untrust 三个安全区域。其中，Trust 安全区域部署内部用户，DMZ 安全区域部署对外服务器，Untrust 安全区域部署外部用户。 Trust 安全区域内的用户通过公网地址访问外部网络。 Untrust 安全区域的用户能够访问 DMZ 安全区域的服务器。

3 Vfw2 为企业 B 提供 UTM 功能。具体功能如下：

- Web 网站控制：禁止访问包含 bt.com 或 bitcom.net 的网站。
- Web 下载控制：禁止下载 AVI 文件。
- FTP 控制：禁止下载 AVI 文件。

实验步骤(CLI)

Setp 1 创建虚拟防火墙 vfw1。

```
< USG> system-view
[USG] ip vpn-instance vfw1
[USG-vpn-vfw1] route-distinguisher 100:1
[USG-vpn-vfw1] quit
```

📖 说明：

创建虚拟防火墙后，需要同时配置路由标识，否则不能进行后续配置。

Setp 2 配置以太网接口。

配置以太网接口 GigabitEthernet 0/0/2

```
[USG] interface GigabitEthernet 0/0/2
[USG-GigabitEthernet0/0/2] ip binding vpn-instance vfw1
[USG-GigabitEthernet0/0/2] ip address 10.1.1.1 24
[USG-GigabitEthernet0/0/2] quit
```

📖 说明：

需要首先配置接口与虚拟防火墙的绑定，再配置接口 IP 地址。如果配置顺序相反，则先配置的地址会被删除。

配置以太网接口 GigabitEthernet 1/0/0

```
[USG] interface GigabitEthernet 1/0/0
[USG-GigabitEthernet1/0/0] ip binding vpn-instance vfw1
[USG-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[USG-GigabitEthernet1/0/0] quit
```

配置以太网接口 GigabitEthernet 1/0/1

```
[USG] interface GigabitEthernet 1/0/1
[USG-GigabitEthernet1/0/1] ip binding vpn-instance vfw1
[USG-GigabitEthernet1/0/1] ip address 2.1.1.1 24
[USG-GigabitEthernet1/0/1] quit
```

Setp 3 配置以太网口加入 vfw1 的安全区域。

配置 GigabitEthernet 0/0/2 加入该 TRUST 安全区域。

```
[USG] firewall zone vpn-instance vfw1 trust
[USG-zone-trust-vfw1] add interface GigabitEthernet 0/0/2
[USG-zone-trust-vfw1] quit
```

配置 GigabitEthernet 1/0/0 加入该 DMZ 安全区域。

```
[USG] firewall zone vpn-instance vfw1 dmz
[USG-zone-dmz-vfw1] add interface GigabitEthernet 1/0/0
[USG-zone-dmz-vfw1] quit
```

配置 GigabitEthernet 1/0/1 加入该 UNTRUST 安全区域。

```
[USG] firewall zone vpn-instance vfw1 untrust
```

```
[USG-zone-untrust-vfw1] add interface GigabitEthernet 1/0/1
[USG-zone-untrust-vfw1] quit
```

说明：

接口与安全区域需要均属于同一虚拟防火墙，否则无法成功将接口加入安全区域。

Setp 4 配置 Trust 安全区域的用户可以通过公网地址访问外部网络。

配置 NAT 地址池。

```
[USG] nat address-group 1 2.1.1.5 2.1.1.10 vpn-instance vfw1
```

配置 Trust 到 Untrust 域间出方向的防火墙策略。

```
[USG] policy interzone vpn-instance vfw1 trust untrust outbound
[USG-policy-interzone-trust-untrust-vfw1-outbound] policy 1
[USG-policy-interzone-trust-untrust-vfw1-outbound-1] policy source 10.1.1.0
0.0.0.255
[USG-policy-interzone-trust-untrust-vfw1-outbound-1] action permit
[USG-policy-interzone-trust-untrust-vfw1-outbound-1] quit
[USG-policy-interzone-trust-untrust-vfw1-outbound] quit
```

配置 Trust 到 Untrust 域间出方向的 NAT 策略。

```
[USG] nat-policy interzone vpn-instance vfw1 trust untrust outbound
[USG-nat-policy-interzone-trust-untrust-vfw1-outbound] policy 1
[USG-nat-policy-interzone-trust-untrust-vfw1-outbound-1] policy source 10.1.1.0
0.0.0.255
[USG-nat-policy-interzone-trust-untrust-vfw1-outbound-1] action source-nat
[USG-nat-policy-interzone-trust-untrust-vfw1-outbound-1] address-group 1
[USG-nat-policy-interzone-trust-untrust-vfw1-outbound-1] quit
[USG-nat-policy-interzone-trust-untrust-vfw1-outbound] quit
```

Setp 5 配置外部网络用户可以访问内部服务器。

配置 vfw1 的内部服务器。

```
[USG] nat server vpn-instance vfw1 zone untrust global 2.1.1.100 inside
192.168.1.2 vpn-instance vfw1
```

此处的内部服务器应属于 VPN 实例 vfw1。

配置 vfw1 的 DMZ 和 Untrust 域间防火墙策略。

```
[USG] policy interzone vpn-instance vfw1 dmz untrust inbound
[USG-policy-interzone-dmz-untrust-vfw1-inbound] policy 1
[USG-policy-interzone-dmz-untrust-vfw1-inbound-1] policy destination 192.168.1.2
0
[USG-policy-interzone-dmz-untrust-vfw1-inbound-1] action permit
[USG-policy-interzone-dmz-untrust-vfw1-inbound-1] quit
[USG-policy-interzone-dmz-untrust-vfw1-inbound] quit
```

Setp 6 配置虚拟防火墙 vfw2。

创建 VPN 实例 vfw2。

```
[USG] ip vpn-instance vfw2
[USG-vpn-vfw2] route-distinguisher 100:2
[USG-vpn-vfw2] quit
```

配置 GigabitEthernet 0/0/3 绑定 VPN 实例 vfw2。

```
[USG] interface GigabitEthernet 0/0/3
[USG-GigabitEthernet0/0/3] ip binding vpn-instance vfw2
[USG-GigabitEthernet0/0/3] ip address 100.1.1.1 24
[USG-GigabitEthernet0/0/3] quit
```

配置 GigabitEthernet 0/0/1 绑定 VPN 实例 vfw2。

```
[USG] interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1] ip binding vpn-instance vfw2
[USG-GigabitEthernet0/0/1] ip address 200.1.1.1 24
[USG-GigabitEthernet0/0/1] quit
```

配置 GigabitEthernet 0/0/3 加入该 Trust 安全区域。

```
[USG] firewall zone vpn-instance vfw2 trust
[USG-zone-trust-vfw2] add interface GigabitEthernet 0/0/3
[USG-zone-trust-vfw2] quit
```

配置 GigabitEthernet 0/0/1 加入该 DMZ 安全区域。

```
[USG] firewall zone vpn-instance vfw2 untrust
[USG-zone-dmz-vfw2] add interface GigabitEthernet 0/0/1
[USG-zone-dmz-vfw2] quit
```

Setp 7 配置路由，使防火墙可以连接 internet。

```
[USG]ip route-static vpn-instance vfw2 0.0.0.0 0.0.0.0 192.168.100.254
```

Setp 8 配置 DNS 服务器，保证内网用户可以链接上互联网。

```
[USG]dns server 210.21.196.6
```

Setp 9 配置虚拟防火墙 vfw2 的 Web 过滤。

创建 URL 模式组 bt，将 bt.com、bitcom.net 加入到公共模式组中，匹配方式为任意匹配。

```
[USG] pattern-group bt type url vpn-instance a
[USG-pattern-group-url-bt-a] pattern any bt.com
[USG-pattern-group-url-bt-a] pattern any bitcom.net
[USG-pattern-group-url-bt-a] quit
```

创建文件扩展名模式组 download，将关键字 AVI 加入到公共模式组中。

```
[USG] pattern-group download type file-extension vpn-instance a
[USG-pattern-group-fe-download-a] pattern avi
[USG-pattern-group-fe-download-a] quit
[USG] pattern configure commit
```

Setp 10 配置虚拟防火墙 vfw2 的 URL 过滤。

启用 URL 过滤功能。

[USG] **url-filter enable**

创建 URL 策略 urlpolicy，启用黑白名单，引用公共模式组 bt。

[USG] **url-filter policy urlpolicy vpn-instance a**
[USG-urlfilter-policy-urlpolicy-a] **blacklist enable**
[USG-urlfilter-policy-urlpolicy-a] **blacklist group bt**
[USG-urlfilter-policy-urlpolicy-a] **default action permit**
[USG-urlfilter-policy-urlpolicy-a] **quit**

创建 Web 策略 webpolicy，引用 URL 策略。

[USG] **web-filter policy webpolicy vpn-instance a**
[USG-web-filter-policy-webpolicy-a] **policy url-filter urlpolicy**

启用 Web 内容过滤，实现 Web 下载控制。

[USG-web-filter-policy-webpolicy-a] **web-content enable**
[USG-web-filter-policy-webpolicy-a] **web-content download file-extension group download action block**
[USG-web-filter-policy-webpolicy-a] **quit**

Setp 11 配置虚拟防火墙 vfw2 的 FTP 过滤。

创建 FTP 过滤策略。

[USG] **ftp-filter policy ftppolicy vpn-instance a**

引用公共模式组 download。禁止下载文件类型为 AVI 的文件。

[USG-ftp-filter-policy-ftppolicy-a] **download file-type group download action block**
[USG-ftp-filter-policy-ftppolicy-a] **quit**

在虚拟防火墙 vfw2 的域间应用 UTM 策略。

📖 说明：

由于访问的连接一般是由内网 PC 发起的，所以 UTM 策略应用在 Trust 到 Untrust 的 Outbound 方向。

在域间应用 UTM 策略。

[USG] **policy interzone vpn-instance vfw2 trust untrust outbound**
[USG-policy-interzone-trust-untrust-a-outbound] **policy 0**
[USG-policy-interzone-trust-untrust-a-outbound-0] **action permit**
[USG-policy-interzone-trust-untrust-a-outbound-0] **policy web-filter webpolicy**
[USG-policy-interzone-trust-untrust-a-outbound-0] **policy ftp-filter ftppolicy**
[USG-policy-interzone-trust-untrust-a-outbound-0] **quit**
[USG-policy-interzone-trust-untrust-a-outbound] **quit**

配置 NAT outbound，使内网用户可以访问 Internet。

[USG] **nat address-group 2 192.168.100.150 192.168.100.160 vpn-instance vfw2**
[USG] **nat-policy interzone vpn-instance vfw2 trust untrust outbound**
[USG-nat-policy-interzone-trust-untrust-a-outbound] **policy 0**
[USG-nat-policy-interzone-trust-untrust-a-outbound-0] **policy source 100.1.1.0 0.0.0.255**

```
[USG-nat-policy-interzone-trust-untrust-a-outbound-0] action source-nat
[USG-nat-policy-interzone-trust-untrust-a-outbound-0] address-group 2
[USG-nat-policy-interzone-trust-untrust-a-outbound-0] quit
[USG-nat-policy-interzone-trust-untrust-a-outbound] quit
```

实验步骤(Web)

Setp 1 创建虚拟防火墙 vfw1。

系统 > 虚拟防火墙 > 虚拟防火墙

新建虚拟防火墙

虚拟防火墙名称 vfw1 *
路由标识类型 ASN
路由标识 100 : 1 *<0-65535>:<0-4294967295>
描述

上网用户资源分配

应用 返回

Setp 2 配置各接口 IP 地址并将其加入虚拟防火墙 vfw1 的安全区域中。

网络 > 接口 > 接口

修改GigabitEthernet

接口名称 GigabitEthernet0/0/2 *
别名
VPN实例 vfw1 *
安全区域 trust
模式 路由 交换
连接类型 静态IP DHCP PPPoE
IP地址 10 . 1 . 1 . 1 IP地址详细配置
子网掩码 255 . 255 . 255 . 0
默认网关 . . .

网络 > 接口 > 接口

修改GigabitEthernet

接口名称	GigabitEthernet1/0/0 *
别名	
VPN实例	vfw1 *
安全区域	dmz
模式	◉ 路由 ○ 交换
连接类型	◉ 静态IP ○ DHCP ○ PPPoE
IP地址	192 . 168 . 1 . 1 [IP地址详细配置]
子网掩码	255 . 255 . 255 . 0
默认网关	. . .

网络 > 接口 > 接口

修改GigabitEthernet

接口名称	GigabitEthernet1/0/1 *
别名	
VPN实例	vfw1 *
安全区域	untrust
模式	◉ 路由 ○ 交换
连接类型	◉ 静态IP ○ DHCP ○ PPPoE
IP地址	2 . 1 . 1 . 1 [IP地址详细配置]
子网掩码	255 . 255 . 255 . 0
默认网关	. . .

Setp 3 将 web 配置界面视图切换至 vfw1。



Setp 4 配置虚拟防火墙域间包过滤转发策略。

防火墙 > 安全策略 > 转发策略

新建转发策略

字段	值
源安全区域	trust *
目的安全区域	untrust *
源地址	10.1.1.0/24 (多选)
目的地址	请选择或输入IP地址 (多选)
用户	请选择或输入用户或用户组 (多选)
服务	请选择服务 (多选)
时间段	all
动作	permit *
描述	

Setp 5 配置 NAT 策略使虚拟防火墙 trust 安全区域的用户可以通过公网地址访问外部网络

防火墙 > NAT > 源NAT

源NAT NAT地址池

新建NAT地址池

字段	值
地址池号	1 *<0-1023>
地址池名称	
起始IP	2 . 1 . 1 . 5 *
结束IP	2 . 1 . 1 . 10 *

应用 返回

防火墙 > NAT > 源NAT

源NAT | NAT地址池

新建源NAT

源安全区域 trust *
目的安全区域 untrust *
源地址 10.1.1.0/24 多选
目的地址 请选择或输入IP地址 多选
动作 NAT转换 *
描述

将源地址转换为 地址池中的地址 接口IP地址
地址池 1 *
允许端口地址转换

应用 返回

Setp 6 配置 NAT server

防火墙 > NAT > 虚拟服务器

新建虚拟服务器

映射方式 一对一地址映射
外部地址 2.1.1.100 *
内部地址 192 . 168 . 1 . 2 *
端口转换

应用 返回

Setp 7 配置安全转发策略使外部网络用户可以访问内部虚拟服务器

防火墙 > 安全策略 > 转发策略

新建转发策略

源安全区域	untrust *	
目的安全区域	dmz *	
源地址	请选择或输入IP地址	多选
目的地址	192.168.1.2/32	多选
用户	请选择或输入用户或用户组	多选
服务	请选择服务	多选
时间段	all	
动作	permit *	
描述		

Setp 8 创建虚拟防火墙 vfw2。创建新的虚拟防火墙时，需要切换到根防火墙视图下创建。

系统 > 虚拟防火墙 > 虚拟防火墙

新建虚拟防火墙

虚拟防火墙名称	vfw2 *
路由标识类型	ASN
路由标识	100 : 2 *<0-65535>:<0-4294967295>
描述	

上网用户资源分配

应用 返回

Setp 9 将相应接口与虚拟防火墙 vfw2 绑定，具体步骤省略。

Setp 10 配置静态路由，使防火墙可以连接 internet

路由 > 静态 > 静态路由

新建静态路由

目的地址	0 . 0 . 0 . 0 *
掩码	0 . 0 . 0 . 0 *
下一跳	192 . 168 . 100 . 254 下一跳和接口不能同时为空
目的VPN实例	vfw2
下一跳VPN实例	public
接口	----- NONE -----
IP Link号	----- NONE -----
优先级	60 <1-255>

应用 返回

Setp 11 配置 DNS 服务器。

网络 > DNS > DNS

服务器列表

删除 刷新 | 210 . 21 . 196 . 6 添加

Setp 12 配置虚拟防火墙 vfw2 的 web 过滤。

UTM > 对象 > URL地址组

新建URL地址组

组名	bt *
描述	

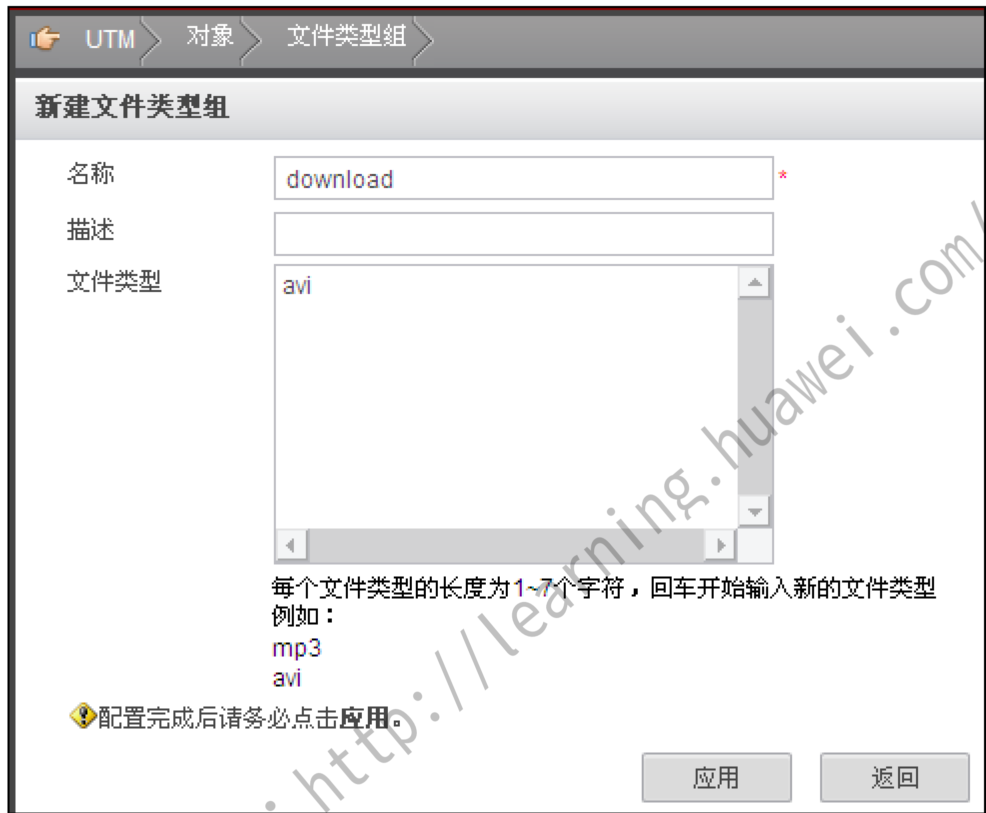
应用 返回

新建URL地址

匹配方式	后缀
内容	bitcom.net *

确定 取消





Setp 13 配置虚拟防火墙 vfw2 的 URL 过滤。

\# 启用 URL 过滤功能。



\# 创建 URL 策略 urlpolicy，启用黑白名单，引用公共模式组 bt。

UTM Web过滤 URL过滤器

新建URL过滤器

名称 urlpolicy *

描述

应用 返回

黑名单配置

选择URL对象组或者在已选框中新建URL组

可选 已选

请输入对象组名称 查询 刷新 新建

bt

应用 返回

UTM Web过滤 URL过滤器

修改URL过滤器

名称 urlpolicy *

描述 URL policy

默认动作 允许

启用URL白名单 启用URL黑名单

启用自定义分类过滤 启用预定义分类过滤

控制选项	控制内容	修改
URL白名单		
URL黑名单	bt	

\# 启用 Web 内容过滤，实现 Web 下载控制。

UTM > Web过滤 > 策略

新建Web过滤策略

名称 download *

描述

应用 返回

新建文件类型组

名称 Download *

描述

文件类型 avi

每个文件类型的长度为1~7个字符，回车开始输入新的文件类型
例如：
mp3
avi

确定 取消




启用Web内容过滤

过滤选项	告警处理对象组	阻断处理对象组	修改
网页浏览关键字			
HTTP POST关键字			
上传文件名称关键字			
下载文件名称关键字			
上传文件类型		download	
下载文件类型		download	

Setp 14 配置虚拟防火墙 vfw2 的 FTP 过滤。

启用 FTP 过滤功能。



新建 FTP 过滤策略。

UTM > FTP过滤 > 策略

新建FTP过滤策略

名称 ftppolicy *

描述

应用 返回

引用公共模式组 download。禁止下载文件类型为 AVI 的文件。

文件类型配置

新建 请输入对象组名 查询 刷新

对象组名称	处理动作
全部文件类型组	----
download	阻断

确定 取消

在域间应用 UTM 策略。

防火墙 > 安全策略 > 转发策略

源安全区域	trust *
目的安全区域	untrust *
源地址	请选择或输入IP地址 [多选]
目的地址	请选择或输入IP地址 [多选]
用户	请选择或输入用户或用户组 [多选]
服务	请选择服务 [多选]
时间段	all
动作	permit *
描述	

☐ IPS

☐ AV

☑ Web过滤

Web过滤策略 download

☐ 邮件过滤

☑ FTP过滤

FTP过滤策略 ftppolicy

配置 NAT outbound，使内网用户可以访问 Internet。

防火墙 > NAT > 源NAT

源NAT | NAT地址池

新建NAT地址池

地址池号	2 *<0-1023>
地址池名称	
起始IP	192.168.100.150 *
结束IP	192.168.100.160 *

[应用] [返回]

验证结果

验证虚拟防火墙 vfw1

1. 从 PC1 ping PC2，在防火墙上运行 display firewall session table，查看 NAT 地址转换情况。
2. 从 PC3 ping NAT server 地址 2.1.1.100，在防火墙上运行 display firewall session table，查看 NAT 地址转换情况。

验证虚拟防火墙 vfw2

Setp 1 在 PC 上访问 www.bt.com， 将会出现“The URL Blacklist is filtered”字样。

6 防火墙高级 VPN 技术

6.1 点到多点IPSec VPN实验

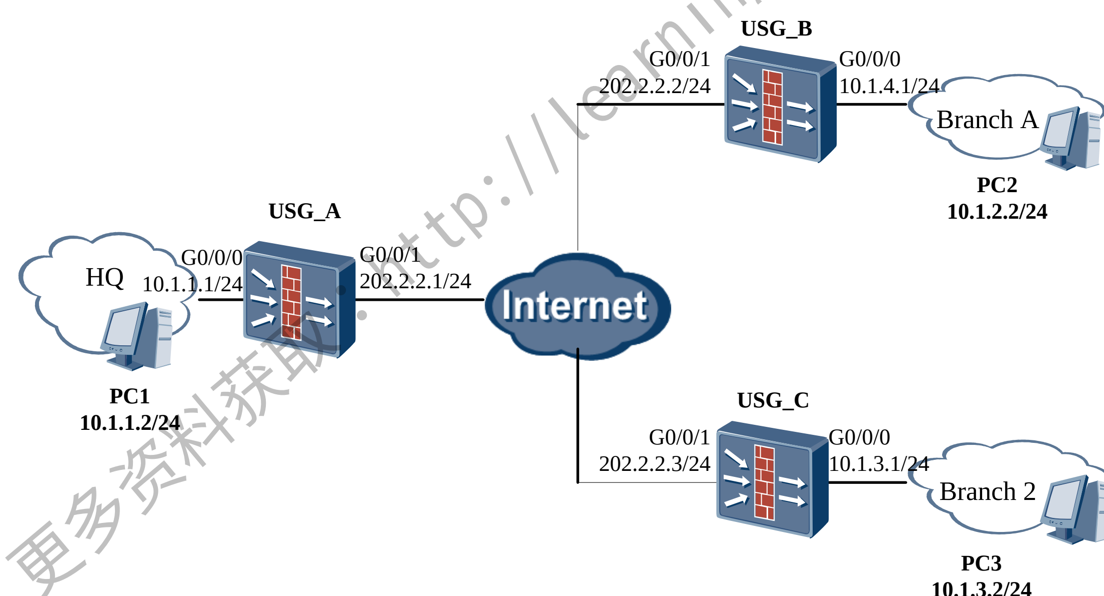
实验目的

掌握 IPSec 点到多点 SA 策略模板方式配置

组网设备

PC 主机 3 台、USG 5000 系列防火墙 3 台、三层交换机 1 台。

实验拓扑图



- 总部 FWA 为固定公网地址, FWB FWC 为动态公网 IP(实验环境配置静态 IP 模拟动态 IP,不影响 IPSEC 的配置,现网可能是通过 ADSL 或 PPPOE 获得的 IP)。
- 分支机构 PC2 PC3 与能与总部 PC1 之间进行安全通信，在 PC2 PC3 与 PC1 能够安全通信之后,PC2 PC3 能够通过 FWA 进行安全通信,FWA 与 FWB FWC 之间使用 IKE 野蛮模式建立安全通道, FWB FWC 不直接建立任何 IPSEC 连接。
- 在 FWA A 和 FWB FWC 上均配置序列号为 10 的 IKE 提议。
- 为使用 pre-shared key 验证方法的提议配置验证字。

实验步骤(命令行)

Setp 1 三层交换机的配置

配置三个三层接口 IP（VLANIF），分别与防火墙 A、B、C 出口 IP 地址在同一网段，三个防火墙的缺省路由下一跳皆分别指向这三个三层接口 IP（VLANIF）。

Setp 2 防火墙 A 基本配置,包括 IP 地址,安全域。

各个接口的 IP 地址及加入域的配置略，请根据具体组网情况配置。

配置到达分支机构的静态路由

[FWA]**ip route-static 0.0.0.0 0.0.0.0 200.0.0.2**

定义用于包过滤和加密的数据流, ACL3000 定义到所有分支机构 FWB FWC 网段的数据流, Soure 定义为总部，destination 定义为各个分支的明细网段。

[FWA]**acl 3000**

[FWA-acl-adv-3000] **rule permit ip source 10.0.0.0 0.0.0.255 destination 10.0.1.0 0.0.0.255**

[FWA-acl-adv-3000] **rule permit ip source 10.0.0.0 0.0.0.255 destination 10.0.2.0 0.0.0.255**

配置 trust 与 untrust 域间包过滤规则

[FWA]**firewall packet-filter default permit interzone trust untrust**

配置 untrust 与 local 域间包过滤规则

[FWA]**firewall packet-filter default permit interzone local untrust**

📖 说明：

Trust 和 untrust 的域间规则可以配置默认放开,也可以配置用 ACL 来放开. 配置 Local 和 Untrust 域间缺省包过滤规则的目的为允许 IPSec 隧道两端设备通信，使其能够协商 SA。

Setp 3 防火墙 A 配置 IPSec 安全提议

创建名为 tran1 的 IPSec 提议。

[FWA]**IPSec proposal tran1**

[FWA-IPSec-proposal-tran1]**transform esp**

[FWA-IPSec-proposal-tran1]**encapsulation-mode tunnel**

[FWA-IPSec-proposal-tran1]**esp authentication-algorithm md5**

[FWA-IPSec-proposal-tran1]**esp encryption-algorithm des**

Setp 4 防火墙 A 配置 IKE 提议

[FWA] **ike proposal 10**

[FWA-ike-proposal-10] **authentication-method pre-share**

[FWA-ike-proposal-10] **authentication-algorithm sha1**

[FWA-ike-proposal-10] **sa duration 86400**

Setp 5 防火墙 A 配置 IKE Peer

创建名为 a 的 IKE peer

[FWA] **ike peer a**

```
[FWA-ike-peer-a] ike-proposal 10
[FWA-ike-peer-a] exchange-mode aggressive
[FWA-ike-peer-a] pre-shared-key huawei
```

📖 说明：

验证字的配置需要与对端设备相同。

Setp 6 防火墙 A 配置安全策略模板

创建安全策略模板 map1tmp。

```
[FWA] IPSec policy-template map1tmp 10
[FWA-IPSec-policy-templet-map1tmp-10] ike-peer a
[FWA-IPSec-policy-templet-map1tmp-10] proposal tran1
[FWA-IPSec-policy-templet-map1tmp-10] security acl 3000
[FWA-IPSec-policy-templet-map1tmp-10] quit
```

创建 IPSEC 安全策略 map1

```
[FWA] IPSec policy map1 10 isakmp template map1tmp
```

Setp 7 防火墙 A 引用安全策略

```
[FWA] interface Ethernet 1/0/0
[FWA-Ethernet1/0/0] IPSec policy map1
```

Setp 8 防火墙 B 基本配置,包括 IP 地址,安全域。

各个接口的 IP 地址及加入域的配置略，请根据具体组网情况配置。

配置到达总部和其他私网的静态路由

```
[FWB]ip route-static 0.0.0.0 0.0.0.0 200.0.1.2
```

定义用于包过滤和加密的数据流,为了实现和总部及分支的通信,source 定义为分支节点的明细网段,destination 定义为总部和分支的所有网段.

```
[FWB]acl 3000
[FWB-acl-adv-3000] rule    permit ip source 10.0.1.0 0.0.0.255 destination 10.0.0.0
0.255.255.255
[FWB-acl-adv-3000]quit
```

配置域间包过滤规则

```
[FWB]firewall packet-filter default permit interzone trust untrust
[FWB]firewall packet-filter default permit interzone local untrust
```

Setp 9 防火墙 B 配置 IPSec 安全提议

创建名为 tran1 的 IPSec 提议。

```
[FWB]IPSec proposal tran1
[FWB-IPSec-proposal-tran1]transform esp
[FWB-IPSec-proposal-tran1]encapsulation-mode tunnel
[FWB-IPSec-proposal-tran1]esp authentication-algorithm md5
[FWB-IPSec-proposal-tran1]esp encryption-algorithm des
```

```
[FWB-IPSec-proposal-tran1]quit
```

Setp 10 防火墙 B 配置 IKE 提议。

```
[FWB] ike proposal 10
[FWB-ike-proposal-10] authentication-method pre-share
[FWB-ike-proposal-10] authentication-algorithm sha1
[FWB-ike-proposal-10] sa duration 86400
```

Setp 11 防火墙 B 配置 IKE Peer

创建名为 b 的 IKE peer

```
[FWB] ike peer b
[FWB-ike-peer-b] ike-proposal 10
[FWB-ike-peer-b] exchange-mode aggressive
[FWB-ike-peer-b] remote-address 200.0.0.1
[FWB-ike-peer-b] pre-shared-key huawei
```

Setp 12 防火墙 B 配置安全策略

```
[FWB] IPSec policy map1 10 isakmp
[FWB-IPSec-policy-isakmp-map1-10] ike-peer b
[FWB-IPSec-policy-isakmp-map1-10] proposal tran1
[FWB-IPSec-policy-isakmp-map1-10] security acl 3000
[FWB-IPSec-policy-isakmp-map1-10] quit
```

Setp 13 防火墙 B 引用安全策略

```
[FWB] interface Ethernet 1/0/0
[FWB-Ethernet1/0/0] IPSec policy map1
```

Setp 14 FWC 的配置

FWC 除 ACL 3000 的源地址、默认路由、接口 IP 地址不同外，其他与 FWB 一致。

实验步骤(Web)

1. Configure USG A.

- 配置各接口 IP 地址并将其加入相应的安全区域。

网络 > 接口 > 接口

修改GigabitEthernet

接口名称 GigabitEthernet0/0/0 *

别名

VPN实例 public *

安全区域 trust

模式 ◉ 路由 ○ 交换

连接类型 ◉ 静态IP ○ DHCP ○ PPPoE

IP地址 10 . 1 . 1 . 1 IP地址详细配置

子网掩码 255 . 255 . 255 . 0

默认网关 . . .

网络 > 接口 > 接口

修改GigabitEthernet

接口名称 GigabitEthernet0/0/1 *

别名

VPN实例 public *

安全区域 untrust

模式 ◉ 路由 ○ 交换

连接类型 ◉ 静态IP ○ DHCP ○ PPPoE

IP地址 202 . 2 . 2 . 1 IP地址详细配置

子网掩码 255 . 255 . 255 . 0

默认网关 . . .

- 配置从总部到达网络 B 和网络 C 的域间安全转发策略。以下显示出了从总部到达网络 B 的转发策略，到达网络 C 的策略类似，此处省略。

Untrust->trust

防火墙 > 安全策略 > 转发策略

修改转发策略

源安全区域	untrust *
目的安全区域	trust *
源地址	any
目的地址	any
用户	请选择或输入用户或用户组
服务	请选择服务
时间段	all
动作	permit *

应用　返回

Trust->Untrust

防火墙 > 安全策略 > 转发策略

修改转发策略

源安全区域	trust *
目的安全区域	untrust *
源地址	any
目的地址	any
用户	any
服务	请选择服务
时间段	all
动作	permit *

应用　返回

- 配置本地策略，允许 untrust 区域与 local 区域的通信。配置 Local 和 Untrust 域间缺省包过滤规则的目的为允许 IPSec 隧道两端设备通信，使其能够协商 SA。

防火墙 > 安全策略 > 本地策略

修改对设备访问控制

源安全区域	untrust *
源地址	any
服务	请选择服务
时间段	all
动作	permit *

应用 返回

- 配置到达网络 B 和网络 C 的静态路由。

路由 > 静态 > 静态路由

新建静态路由

目的地址	0 . 0 . 0 . 0 *
掩码	0 . 0 . 0 . 0 *
下一跳	202 . 2 . 2 . 2 下一跳和接口不能同时为空
接口	----- NONE -----
IP Link号	----- NONE -----
优先级	60 <1-255>

应用 返回

路由 > 静态 > 静态路由

新建静态路由

目的地址	0 . 0 . 0 . 0 *
掩码	0 . 0 . 0 . 0 *
下一跳	202 . 2 . 2 . 3 下一跳和接口不能同时为空
接口	----- NONE -----
IP Link号	----- NONE -----
优先级	60 <1-255>

应用 返回

- 创建 IKE 协商阶段 1 ，分别命名为 b 和 c，当配置 c 时，需要选择“不指定对端网关”。

VPN > IPSec > IKE协商

新建阶段1

阶段1	b *
版本	V1　V2　● V1 and V2
协商模式	● 主模式　野蛮模式
本地ID类型	IP
预共享密钥	●●●●● *
对端网关配置方式	指定对端网关
对端网关VPN实例	public
对端网关IP	202 . 2 . 2 . 2 * -
对端地址池范围	-
VPN实例	public

+ 高级

应用　返回

VPN > IPSec > IKE协商

新建阶段1

阶段1	c *
版本	V1　V2　● V1 and V2
协商模式	● 主模式　野蛮模式
本地ID类型	IP
预共享密钥	●●●●● *
对端网关配置方式	不指定对端网关
对端地址池范围	-
VPN实例	public

+ 高级

应用　返回

- 配置 IKE 第二阶段协商，引用阶段 1 的配置。

VPN > IPSec > IKE协商

新建阶段2

阶段2	map1 * - 10	*<1-10000>
阶段1	b	
备份阶段1	不指定备份阶段1	
本端网关IP	202 . 2 . 2 . 1	

+ 高级

应用 返回

VPN > IPSec > IKE协商

新建阶段2

阶段2	map_temp * - 1	*<1-10000>
阶段1	c	

+ 高级

应用 返回

- 新建 IPSec 策略。

VPN > IPSec > IPSec策略

新建IPSec策略

IPSec策略	map1-10 *
数据流配置方式	● 指定数据流 ○ L2TP over IPSec
源地址	10.1.1.0/24
目的地址	10.1.2.0/24
服务	ip
动作	permit

应用 返回

- 将 IPSec 策略应用到接口上，点击"应用接口：- NONE -"，选择 GE0/0/1 接口。

2. **Configure USG B.**

- 配置各接口 IP 地址并将其加入相应的安全区域。配置请参考 USG A，此处省略具体步骤。
- 配置域间安全转发策略。

Untrust->Trust

防火墙 > 安全策略 > 转发策略 >

修改转发策略

源安全区域	untrust *
目的安全区域	trust *
源地址	any
目的地址	any
用户	请选择或输入用户或用户组
服务	请选择服务
时间段	all
动作	permit *

应用 返回

Trust->Untrust

防火墙 > 安全策略 > 转发策略 >

修改转发策略

源安全区域	trust *
目的安全区域	untrust *
源地址	any
目的地址	any
用户	any
服务	请选择服务
时间段	all
动作	permit *

应用 返回

- 配置本地策略，允许 untrust 区域与 local 区域的通信。

防火墙 > 安全策略 > 本地策略

修改对设备访问控制

源安全区域 untrust *
源地址 any
服务 请选择服务
时间段 all
动作 permit *

应用 返回

- 配置到达网络 A 的静态路由，此处下一跳地址为 202.2.2.1。

路由 > 静态 > 静态路由

新建静态路由

目的地址 0 . 0 . 0 . 0 *
掩码 0 . 0 . 0 . 0 *
下一跳 202 . 2 . 2 . 1 下一跳和接口不能同时为空
接口 ----- NONE -----
IP Link号 ----- NONE -----
优先级 60 <1-255>

应用 返回

- 配置第一阶段的 IKE 协商参数，新建名为 a 的 IKE peer。

VPN > IPSec > IKE协商

新建阶段1

阶段1 a *

版本 V1 V2 V1 and V2

协商模式 主模式 野蛮模式

本地ID类型 IP

预共享密钥 ●●●●● *

对端网关配置方式 指定对端网关

对端网关VPN实例 public

对端网关IP 202 . 2 . 2 . 1 * -

对端地址池范围 -

VPN实例 public

高级

应用 返回

- 配置第二阶段的 IKE 协商参数，引用第一阶段配置。

VPN > IPSec > IKE协商

新建阶段2

阶段2 map1 * - 10 *<1-10000>

阶段1 a

备份阶段1 不指定备份阶段1

本端网关IP 202 . 2 . 2 . 2

高级

应用 返回

- 新建 IPSec 策略，将 IKE 配置参数引用到策略中。

● 将 IPSec 策略应用到接口上，点击" 应用接口：- NONE - "，选择 GE0/0/1 接口。

3. Configure USG C. (Omit)

● USG C 的配置请参考 USG B 的配置。

验证结果

PC2 PC3 可以访问 PC1,之后 PC1 能够访问到 PC2 PC3,注意在 IPSEC SA 建立之前, PC1 不能主动访问 PC2 PC3, PC2 PC3 也不能互访.IPSEC SA 只能由分支节点触发.

总部防火墙 FWA 上可以查看到两对 IKE SA, phase 1 表示 IKE 协商, phase2 表示 IPSEC SA 协商。

```
[FWA]display ike sa
    connection-id   peer              vpn    flag         phase    doi
  --------------------------------------------------------------
```

```
         10          200.0.2.1      0     RD              1      IPSEC
          8          200.0.1.1      0     RD              1      IPSEC
         11          200.0.2.1      0     RD              2      IPSEC
          9          200.0.1.1      0     RD              2      IPSEC
flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```

分支上 FWB 可以查看到总部 peer 的 IKE phase 1 和 phase 2

```
<FWB>display ike sa
    connection-id   peer              flag          phase    doi
  ------------------------------------------------------------
         13          200.0.0.1      RD|ST          1       IPSEC
         14          200.0.0.1      RD|ST          2       IPSEC
```

6.2 NAT穿越实验

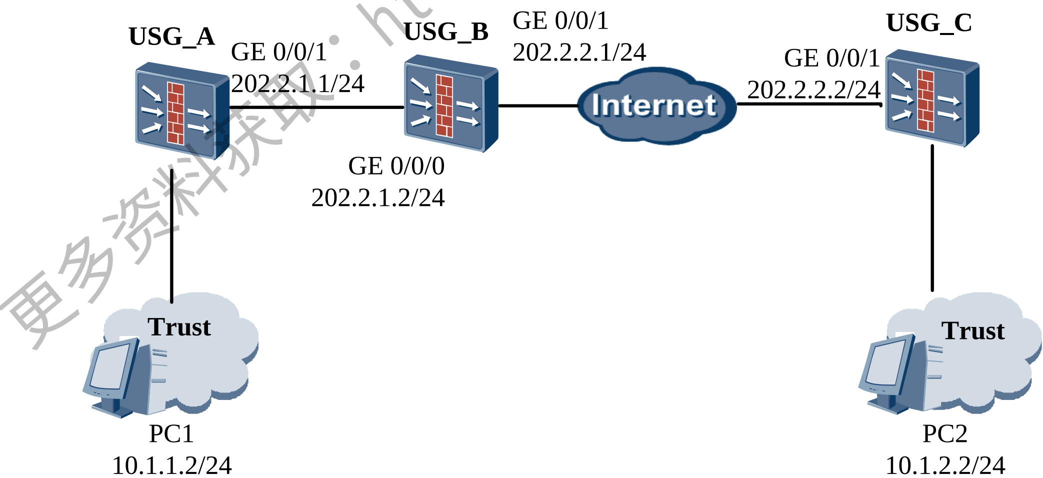
实验目的

掌握 IPSec NAT 穿越策略模板配置

组网设备

PC 主机 2 台、USG 5000 系列防火墙 3 台

实验拓扑图



- PC1 发起 IPSEC 连接,能与 PC2 之间进行安全通信，在 USG_A 与 USG_C 之间使用 IKE 野蛮模式自动协商+策略模板建立安全通道。
- PC1 可以访问公网。
- 在 USG_A 和 USG_B 上均配置序列号为 10 的 IKE 提议。
- 为使用 pre-shared key 验证方法的提议配置验证字。

- USG_A 为固定公网地址，USG_B 的公网 IP 地址与 IPSEC 配置无关，USG_C 为内网地址，动静态无关。

实验步骤(命令行)

Setp 1 整体网络搭建

防火墙 A、B、C 之间需保证互通。防火墙 B 配置 NAT 后，需保证防火墙 C 能够在做地址转换后与防火墙 A 互通。防火墙 B 只需做普通 NAT 配置。

Setp 2 防火墙 A 基本配置，包括 IP 地址及路由

配置到达其他分支节点的静态路由

```
[USG_A]ip route-static 0.0.0.0 0.0.0.0 200.0.0.2
```

定义用于包过滤和加密的数据流，在模板方式下，总部只建立一个 ACL，ACL 的源可以定义包括总部和分支的所有网段，用于分支网点的互通。目的是各分支机构的明细路由，对于每一个分支机构，建议配置一个 rule。

```
[USG_A]acl 3000
[USG_A-acl-adv-3000]rule permit ip source 10.0.0.0 0.0.0.255 destination 10.0.1.0 0.0.0.255
```

配置域间包过滤规则

```
[USG_A]firewall packet-filter default permit interzone trust untrust
[USG_A]firewall packet-filter default permit interzone local untrust
```

Trust 和 untrust 的域间规则需要配置默认放开。 配置 Local 和 Untrust 域间缺省包过滤规则的目的为允许 IPSec 隧道两端设备通信，使其能够协商 SA。

Setp 3 防火墙 A 配置 IPSec 安全提议

配置 IKE 本地名称

```
[USG_A] ike local-name USG_A
```

创建名为 tran1 的 IPSec 提议。

```
[USG_A]IPSec proposal tran1
[USG_A-IPSec-proposal-tran1]transform esp
[USG_A-IPSec-proposal-tran1]encapsulation-mode tunnel
[USG_A-IPSec-proposal-tran1]esp authentication-algorithm md5
[USG_A-IPSec-proposal-tran1]esp encryption-algorithm des
[USG_A-IPSec-proposal-tran1]quit
```

以上配置参数为缺省参数，可以不配置

Setp 4 防火墙 A 配置 IKE 提议。

```
[USG_A] ike proposal 10
[USG_A-ike-proposal-10] authentication-method pre-share
[USG_A-ike-proposal-10] authentication-algorithm sha1
[USG_A-ike-proposal-10] sa duration 86400
[USG_A-ike-proposal-10] quit
```

86400 秒为默认 ISAKMP SA 的生存周期

Setp 5 防火墙 A 配置 IKE Peer

\# 创建名为 a 的 IKE peer，模板方式下，只需要创建一个 peer

[USG_A] **ike peer a**
[USG_A-ike-peer-a] **ike-proposal 10**
[USG_A-ike-peer-a] **pre-shared-key Huawei**
[USG_A-ike-peer-a] **local-id-type name**
[USG_A-ike-peer-a] **remote-name FWC**
[USG_A-ike-peer-a] **exchange-mode aggressive**

\# 配置 NAT 穿越。

[USG_A-ike-peer-a] **nat traversal**
[USG_A-ike-peer-a] **quit**

验证字的配置需要与对端设备相同。

Setp 6 防火墙 A 配置安全策略模板

\# 创建安全策略模板 map1tmp

[USG_A]**IPSec policy-template map1tmp 10**
[USG_A-IPSec-policy-templet-map1tmp-10] **ike-peer a**
[USG_A-IPSec-policy-templet-map1tmp-10] **proposal tran1**
[USG_A-IPSec-policy-templet-map1tmp-10] **security acl 3000**
[USG_A-IPSec-policy-templet-map1tmp-10] **quit**

\#创建安全策略,引用策略模板

[USG_A]**IPSec policy map1 10 isakmp template map1tmp**

Setp 7 防火墙 A 引用安全策略

[USG_A] **interface Ethernet 1/0/0**
[USG_A-Ethernet1/0/0] **IPSec policy map1**

Setp 8 防火墙 C 基本配置，包括 IP 地址及路由

\# 配置到达总部和其他分支节点的静态路由

[USG_C]**ip route-static 0.0.0.0 0.0.0.0 200.0.2.2**

\# 定义用于包过滤和加密的数据流,分支 ACL 的源定义为分支明细网段,destination 定义包括总部和分支的所有网段,用于和总部及其他分支网点的互通.对于每一个分支机构,建议配置一个 ACL 即可.

[USG_C]**acl 3000**
[USG_C-acl-adv-3000] **rule permit ip source 10.0.1.0 0.0.0.255 destination 10.0.0.0 0.0.0.255**

\# 配置 trust 与 untrust 域间包过滤规则

[USG_C]**firewall packet-filter default permit interzone trust untrust**

\# 配置 untrust 与 local 域间包过滤规则

[USG_C]**firewall packet-filter default permit interzone local untrust**

Trust 和 untrust 的域间可以配置默认放开,也可以配置 ACL 放开. 配置 Local 和 Untrust 域间缺省包过滤规则的目的为允许 IPSec 隧道两端设备通信，使其能够协商 SA。

Setp 9 防火墙 C 配置 IPSec 安全提议

\# 配置 IKE 本地名称

```
[USG_C] ike local-name USG_C
```

\# 创建名为 tran1 的 IPSec 提议。

```
[USG_C]IPSec proposal tran1
[USG_C-IPSec-proposal-tran1]transform esp
[USG_C-IPSec-proposal-tran1]encapsulation-mode tunnel
[USG_C-IPSec-proposal-tran1]esp authentication-algorithm md5
[USG_C-IPSec-proposal-tran1]esp encryption-algorithm des
[USG_C-IPSec-proposal-tran1]quit
```

Setp 10 防火墙 C 配置 IKE 提议。

```
[USG_C] ike proposal 10
[USG_C-ike-proposal-10] authentication-method pre-share
[USG_C-ike-proposal-10] authentication-algorithm sha1
[USG_C-ike-proposal-10] sa duration 86400
[USG_C-ike-proposal-10] quit
```

Setp 11 防火墙 C 配置 IKE Peer

\# 创建名为 c 的 IKE peer, 一个分支节点只需要创建一个 Peer

```
[USG_C] ike peer c
[USG_C-ike-peer-c] ike-proposal 10
[USG_C-ike-peer-c] remote-address 200.0.0.1
[USG_C-ike-peer-c] pre-shared-key Huawei
[USG_C-ike-peer-c] local-id-type name
[USG_C-ike-peer-c] remote-name USG_A
[USG_C-ike-peer-c] exchange-mode aggressive
```

\# 配置 NAT 穿越。

```
[USG_C-ike-peer-c] nat traversal
[USG_C-ike-peer-c] quit
```

验证字的配置需要与对端设备相同。

Setp 12 防火墙 C 配置安全策略

\# 创建安全策略 map1 的子策略 10。

```
[USG_C] IPSec policy map1 10 isakmp
[USG_C-IPSec-policy-isakmp-map1-10] ike-peer c
[USG_C-IPSec-policy-isakmp-map1-10] proposal tran1
[USG_C-IPSec-policy-isakmp-map1-10] security acl 3000
```

```
[USG_C-IPSec-policy-isakmp-map1-10] quit
```

Setp 13 防火墙 C 引用安全策略

```
[USG_C] interface Ethernet 0/0/0
[USG_C-Ethernet0/0/0] IPSec policy map1
```

实验步骤(Web)

Setp 1 整体网络搭建

防火墙 A、B、C 之间需保证互通。防火墙 B 配置 NAT 后，需保证防火墙 C 能够在做地址转换后与防火墙 A 互通。防火墙 B 只需做普通 NAT 配置。

1. 配置防火墙 A

Setp 2 防火墙 A 基本配置，包括 IP 地址及路由。

配置到达其他分支节点的静态路由

路由 > 静态 > 静态路由

新建静态路由

目的地址 0 . 0 . 0 . 0 *
掩码 0 . 0 . 0 . 0 *
下一跳 200 . 0 . 0 . 2 下一跳和接口不能同时为空
接口 ----- NONE -----
IP Link号 ----- NONE -----
优先级 60 <1-255>
应用 返回

配置域间包过滤规则

防火墙 > 安全策略 > 转发策略

修改转发策略

字段	值
源安全区域	untrust *
目的安全区域	trust *
源地址	any
目的地址	any
用户	请选择或输入用户或用户组
服务	请选择服务
时间段	all
动作	permit *

应用 返回

防火墙 > 安全策略 > 转发策略

修改转发策略

字段	值
源安全区域	trust *
目的安全区域	untrust *
源地址	any
目的地址	any
用户	any
服务	请选择服务
时间段	all
动作	permit *

应用 返回

防火墙 > 安全策略 > 本地策略

修改对设备访问控制

源安全区域 untrust
源地址 any
服务 请选择服务
时间段 all
动作 permit

应用 返回

Trust 和 untrust 的域间规则需要配置默认放开。 配置 Local 和 Untrust 域间缺省包过滤规则的目的为允许 IPSec 隧道两端设备通信，使其能够协商 SA。

Setp 3 配置第一阶段的 IKE 协商参数，新建名为 a 的 IKE peer。设置协商模式为野蛮模式，并将本地 ID 类型配置为名称。

VPN > IPSec > IKE协商

新建阶段1

阶段1 a
版本 V1 V2 V1 and V2
协商模式 主模式 野蛮模式
本地ID类型 名称
远端名称 FWC
本地名称 FWA
预共享密钥 •••••
对端网关配置方式 不指定对端网关
对端地址池范围 . . . - . . .
VPN实例 public
高级

应用 返回

Setp 4 在 IKE 第一阶段协商的高级设置下，配置 NAT 穿越功能。

高级

加密算法	DES-CBC	认证算法	SHA1
DH组	DH-Group1		
完整性算法	HMAC-SHA1		
SA超时时间	86400 *<60-604800>秒		
DPD工作模式	----- NONE -----		
NAT穿越	☑ 启动		
对端认证IP地址			

Setp 5 配置第二阶段的 IKE 协商参数，引用第一阶段配置。

VPN > IPSec > IKE协商

新建阶段2

阶段2	map1tmp * - 10 *<1-10000>
阶段1	a

高级

应用 返回

Setp 6 新建 IPSec 策略，将 IKE 配置参数引用到策略中。

VPN > IPSec > IPSec策略

新建IPSec策略

IPSec策略	map1tmp-10 *
数据流配置方式	◉ 指定数据流 ○ L2TP over IPSec
源地址	10.0.0.0/24
目的地址	10.0.1.0/24
服务	ip
动作	permit

应用 返回

Setp 7 将 IPSec 策略应用到接口上，点击” 应用接口：- NONE -”。



2. 配置防火墙 C

Setp 8 防火墙 C 基本配置，包括 IP 地址及路由。

配置到达其他分支节点的静态路由



配置域间包过滤规则

防火墙 > 安全策略 > 转发策略

修改转发策略

字段	值
源安全区域	untrust *
目的安全区域	trust *
源地址	any
目的地址	any
用户	请选择或输入用户或用户组
服务	请选择服务
时间段	all
动作	permit *

应用 返回

防火墙 > 安全策略 > 转发策略

修改转发策略

字段	值
源安全区域	trust *
目的安全区域	untrust *
源地址	any
目的地址	any
用户	any
服务	请选择服务
时间段	all
动作	permit *

应用 返回

防火墙 > 安全策略 > 本地策略

修改对设备访问控制

源安全区域	untrust
源地址	any
服务	请选择服务
时间段	all
动作	permit *

应用　返回

Setp 9　防火墙 C 配置 IPSec 安全提议

VPN > IPSec > IKE协商

新建阶段1

阶段1	c *
版本	○ V1　○ V2　● V1 and V2
协商模式	○ 主模式　● 野蛮模式
本地ID类型	名称
远端名称	FWA *
本地名称	FWC *
预共享密钥	●●●●● *
对端网关配置方式	指定对端网关
对端网关VPN实例	public
对端网关IP	200.0.0.1 * -
对端地址池范围	-
VPN实例	public

高级

应用　返回

Setp 10　在 IKE 第一阶段协商的高级设置下，配置 NAT 穿越功能。

高级

加密算法 DES-CBC　认证算法 SHA1

DH组 DH-Group1

完整性算法 HMAC-SHA1

SA超时时间 86400 *<60-604800>秒

DPD工作模式 ----- NONE -----

NAT穿越 启动

对端认证IP地址

Setp 11 配置第二阶段的 IKE 协商参数，引用第一阶段配置。

VPN > IPSec > IKE协商

新建阶段2

阶段2 map1 * - 10 *<1-10000>

阶段1 c

备份阶段1 不指定备份阶段1

本端网关IP 200 . 0 . 0 . 1

高级

应用　返回

Setp 12 新建 IPSec 策略，将 IKE 配置参数引用到策略中。

VPN > IPSec > IPSec策略

新建IPSec策略

IPSec策略 map1-10 *

数据流配置方式 指定数据流　L2TP over IPSec

源地址 10.0.1.0/24

目的地址 10.0.0.0/24

服务 ip

动作 permit

应用　返回

Setp 13 将 IPSec 策略应用到接口上，点击” 应用接口：- NONE -”。



验证结果

PC2 发起访问,之后 PC1 与 PC2 之间可以相互访问.

PC2 同时可以访问到公网,Ping USG_A 的 200.0.0.1 可以 PING 通,同时在 FWB 上可以查看 NAT 转换 session 表项

```
<USG_B>dis firewall session table
udp:200.0.2.1:500[200.0.1.1:13488]-->200.0.0.1:500
udp:200.0.2.1:4500[200.0.1.1:45488]-->200.0.0.1:4500
```

总部防火墙 USG_A 上可以查看到对应的 IKE SA, phase 1 表示 IKE 协商, phase2 表示 IPSEC SA 协商.

```
<USG_A>display ike sa
    connection-id   peer            vpn    flag        phase    doi
  ----------------------------------------------------------
        1           200.0.1.1        0      RD            1      IPSEC
        5           200.0.1.1        0      RD            2      IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
14:23:36    05-23-2008
```

分支上 USG_C 可以查看到总部 peer 的 IKE phase 1 和 phase 2, USG_C 是发起方,标志位为 ST

```
<USG_C>dis ike sa
    connection-id   peer            flag        phase    doi
  ------------------------------------------------------
        2           200.0.0.1       RD|ST         1      IPSEC
        6           200.0.0.1       RD|ST         2      IPSEC
```

总部防火墙 USG_A 上可以查看到一对双向的 IPSEC SA,对应两个分支 USG_C, nat traversal: Y 表示 IPSEC 的 NAT 穿越生效

```
<USG_A>display IPSec sa

  -----------------------------
  IPSec policy name: "map1"
  sequence number: 10
  mode: template
  vpn: 0
  -----------------------------
    connection id: 5
    encapsulation mode: tunnel
    tunnel local : 200.0.0.1        tunnel remote: 200.0.1.1
    flow            source: 10.0.0.0/255.0.0.0 0/0
    flow destination: 10.0.1.0/255.255.255.0 0/0

    [inbound ESP SAs]
      spi: 3716495275 (0xdd8537ab)
      vpn: 0
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1886658472/1187
      max received sequence-number: 11447
      udp encapsulation used for nat traversal: Y

    [outbound ESP SAs]
      spi: 3704042965 (0xdcc735d5)
      vpn: 0
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1886475336/1187
      max sent sequence-number: 11447
      udp encapsulation used for nat traversal: Y
```


6.3 隧道化链路备份IPSec VPN实验

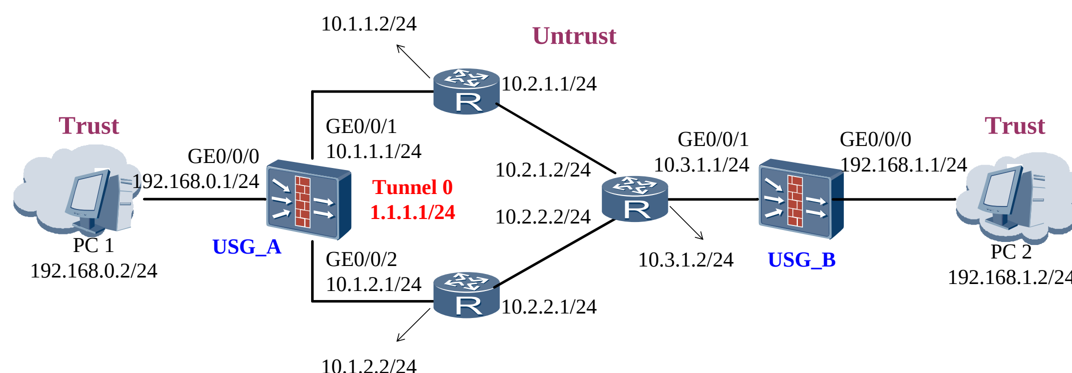
实验目的

该实验介绍如何通过隧道化配置使 IPSec VPN 到达链路备份的作用。

组网设备

PC 机 2 台，USG 系列防火墙 2 台，路由器/三层交换机 3 台。

实验拓扑图



实验步骤(命令行)

配置防火墙 A。

Setp 1 配置各接口 IP 地址并加入安全区域

```
[USG_A] interface GigabitEthernet 0/0/1
[USG_A-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[USG_A-GigabitEthernet0/0/1] quit

[USG_A] interface GigabitEthernet 0/0/2
[USG_A- GigabitEthernet 0/0/2] ip address 10.1.2.1 24
[USG_A- GigabitEthernet 0/0/2] quit

[USG_A] firewall zone untrust
[USG_A-zone-untrust] add interface GigabitEthernet 0/0/1
[USG_A-zone-untrust] add interface GigabitEthernet 0/0/2
[USG_A-zone-untrust] quit
```

Setp 2 配置域间安全转发策略。

```
[USG_A] firewall packet-filter default permit interzone trust untrust
```

Setp 3 创建 tunnel 接口并将其加入 untrust 区域。

```
[USG_A] interface Tunnel 0
[USG_A-Tunnel0] tunnel-protocol ipsec
[USG_A-Tunnel0] ip address 1.1.1.1 24
[USG_A-Tunnel0] quit
[USG_A] firewall zone untrust
[USG_A-zone-untrust] add interface Tunnel 0
[USG_A-zone-untrust] quit
```

Setp 4 定义保护数据流。

```
[USG_A] acl 3000
[USG_A-acl-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
```

Setp 5 配置 IPSec 安全提议和 IKE 安全提议。使用默认参数进行配置。

```
[USG_A] ipsec proposal tran1
[USG_A-ipsec-proposal-tran1] quit
[USG_A] ike proposal 10
[USG_A-ike-proposal-10] quit
```

Setp 6 配置 IKE peer。

```
[USG_A] ike peer b
[USG_A-ike-peer-b] ike-proposal 10
[USG_A-ike-peer-b] remote-address 10.3.1.1
[USG_A-ike-peer-b] pre-shared-key huawei
[USG_A-ike-peer-b] quit
```

Setp 7 创建 IPSec 安全策略 map1。

```
[USG_A] ipsec policy map1 10 isakmp
[USG_A-ipsec-policy-isakmp-map1-10] proposal tran1
[USG_A-ipsec-policy-isakmp-map1-10] security acl 3000
[USG_A-ipsec-policy-isakmp-map1-10] ike-peer b
[USG_A-ipsec-policy-isakmp-map1-10] quit
```

Setp 8 将两个 IPSec 安全策略应用到 tunnel 接口上。

```
[USG_A] interface Tunnel 0
[USG_A- Tunnel 0] ipsec policy map1
[USG_A- Tunnel 0] quit
```

配置防火墙 B。

Setp 9 防火墙 B 的配置与防火墙 A 类似。

```
[USG_B] interface GigabitEthernet 0/0/1
[USG_B-GigabitEthernet0/0/1] ip address 10.3.1.1 24
[USG_B-GigabitEthernet0/0/1] quit

[USG_B] interface GigabitEthernet 0/0/0
[USG_B-GigabitEthernet0/0/0] ip address 192.168.1.1 24
[USG_B-GigabitEthernet0/0/0] quit

[USG_B] firewall zone untrust
[USG_B-zone-untrust] add interface GigabitEthernet 0/0/1
[USG_B-zone-untrust] quit
```

```
[USG_B] firewall packet-filter default permit interzone untrust trust
[USG_B] ip route-static 0.0.0.0 0.0.0.0 10.3.1.2

[USG_B] acl 3000
[USG_B-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
[USG_B-acl-adv-3000] quit
```

IPsec 提议和 IKE 提议均采用默认参数设置。

```
[USG_B] ipsec proposal tran1
[USG_B-ipsec-proposal-tran1] quit
[USG_B] ike proposal 10
[USG_B-ike-proposal-10] quit
```

防火墙上指定对端地址时，需要指定防火墙 tunnel 接口地址。

```
[USG_B] ike peer a
[USG_B-ike-peer-a] remote-address 1.1.1.1
[USG_B-ike-peer-a] ike-proposal 10
[USG_B-ike-peer-a] pre-shared-key huawei
[USG_B-ike-peer-a] quit

[USG_B] ipsec policy map1 10 isakmp
[USG_B-ipsec-policy-isakmp-map1-10] security acl 3000
[USG_B-ipsec-policy-isakmp-map1-10] proposal tran1
[USG_B-ipsec-policy-isakmp-map1-10] ike-peer a
[USG_B-ipsec-policy-isakmp-map1-10] quit

[USG_B] interface GigabitEthernet 0/0/1
[USG_B-GigabitEthernet0/0/1] ipsec policy map1
[USG_B-GigabitEthernet0/0/1] quit
```

配置三台路由器。

Setp 10 在路由器上配置好各接口 IP 地址，并配置 OSPF 通过各接口直连网段，保证三台路由器之间路由可达即可。具体步骤省略。

```
[Router_A] ospf 100
[Router_A-ospf-100] area 0
[Router_A-ospf-100-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[Router_A-ospf-100-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[Router_A-ospf-100-area-0.0.0.0] quit
[Router_A-ospf-100] quit

[Router_B] ospf 100
[Router_B-ospf-100] area 0
```

```
[Router_B-ospf-100-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[Router_B-ospf-100-area-0.0.0.0] network 10.2.2.0 0.0.0.255
[Router_B-ospf-100-area-0.0.0.0] quit
[Router_B-ospf-100] quit

[Router_C] ospf 100
[Router_C-ospf-100] area 0
[Router_C-ospf-100-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[Router_C-ospf-100-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[Router_C-ospf-100-area-0.0.0.0] network 10.2.2.0 0.0.0.255
[Router_C-ospf-100-area-0.0.0.0] quit
[Router_C-ospf-100] quit
```

验证结果

1. 检查从 PC1 是否能 ping 通 PC2，如能 ping 通，在防火墙上运行 display ike sa 和 display ipsec sa 命令，查看是否已经成功建立 IPSec 隧道。
2. 查看当路由器 A 或路由器 B 接口 down 掉时，IPSec 隧道是否还可以正常建立。

6.4 主备链路备份IPSec VPN实验

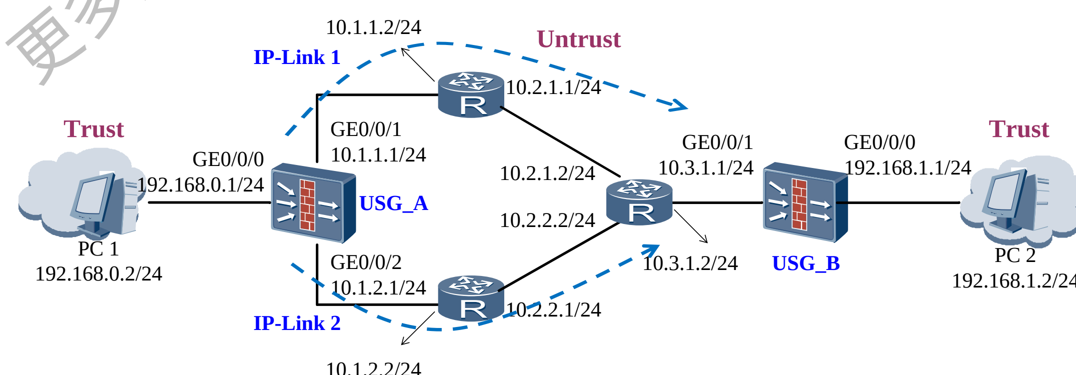
实验目的

使用 IP Link 功能结合 IPSec VPN 组网环境完成 IPSec 主备链路备份，提高系统可靠性。

组网设备

PC 机 2 台，USG 系列防火墙 2 台，路由器/三层交换机 3 台。

实验拓扑图



实验步骤(命令行)

配置防火墙 A。

Setp 1 配置各接口 IP 地址并加入安全区域

```
[USG_A]interface GigabitEthernet 0/0/1
[USG_A-GigabitEthernet0/0/1]ip address 10.1.1.1 24
[USG_A-GigabitEthernet0/0/1]quit

[USG_A]interface GigabitEthernet 0/0/2
[USG_A- GigabitEthernet 0/0/2]ip address 10.1.2.1 24
[USG_A- GigabitEthernet 0/0/2]quit

[USG_A]firewall zone untrust
[USG_A-zone-untrust]add interface GigabitEthernet 0/0/1
[USG_A-zone-untrust]add interface GigabitEthernet 0/0/2
[USG_A-zone-untrust]quit
```

Setp 2 配置域间安全转发策略。

```
[USG_A]firewall packet-filter default permit interzone trust untrust
```

Setp 3 定义保护数据流。由于需要将 IPSec 安全策略分别应用到 USG_A 的两个接口上，因此需要配置两条 ACL，但其内容一致。

```
[USG_A]acl 3000
[USG_A-acl-adv-3000]rule permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
[USG_A]acl 3001
[USG_A-acl-adv-3001]rule permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
```

Setp 4 配置 IPSec 安全提议和 IKE 安全提议。使用默认参数进行配置。

```
[USG_A]ipsec proposal tran1
[USG_A-ipsec-proposal-tran1]quit
[USG_A]ike proposal 10
[USG_A-ike-proposal-10]quit
```

Setp 5 配置 IKE peer。

```
[USG_A]ike peer b
[USG_A-ike-peer-b]ike-proposal 10
[USG_A-ike-peer-b]remote-address 10.3.1.1
[USG_A-ike-peer-b]pre-shared-key huawei
[USG_A-ike-peer-b]quit
```

Setp 6 创建 IPSec 安全策略 map1。

```
[USG_A]ipsec policy map1 10 isakmp
[USG_A-ipsec-policy-isakmp-map1-10]proposal tran1
[USG_A-ipsec-policy-isakmp-map1-10]security acl 3000
[USG_A-ipsec-policy-isakmp-map1-10]ike-peer b
[USG_A-ipsec-policy-isakmp-map1-10]quit
```

Setp 7 创建 IPSec 安全策略 map2。

```
[USG_A]ipsec policy map2 10 isakmp
[USG_A-ipsec-policy-isakmp-map1-10]proposal tran1
[USG_A-ipsec-policy-isakmp-map1-10]security acl 3001
[USG_A-ipsec-policy-isakmp-map1-10]ike-peer b
[USG_A-ipsec-policy-isakmp-map1-10]quit
```

Setp 8 将两个 IPSec 安全策略分别应用到接口上。

```
[USG_A]interface GigabitEthernet 0/0/1
[USG_A-GigabitEthernet0/0/1]ipsec policy map1
[USG_A-GigabitEthernet0/0/1]quit
```

```
[USG_A]interface GigabitEthernet 0/0/2
[USG_A- GigabitEthernet 0/0/2]ipsec policy map2
[USG_A- GigabitEthernet 0/0/2]quit
```

Setp 9 配置 IP-Link 检测远端链路情况。

```
[USG_A] ip-link check enable
[USG_A] ip-link 1 destination 10.2.1.2 mode icmp
[USG_A] ip-link 2 destination 10.2.2.2 mode icmp
```

```
[USG_A]ip route-static 0.0.0.0 0.0.0.0 10.1.1.2 track ip-link 1
[USG_A]ip route-static 0.0.0.0 0.0.0.0 10.1.2.2 preference 70 track ip-link 2
```

配置防火墙 B。

Setp 10 防火墙 B 的配置与防火墙 A 类似。区别在于由于防火墙 A 可以由两个接口发起 IPSec 隧道，因此需要在防火墙 B 上采用 IPSec 策略模板方式进行 IPSec 配置。

```
[USG_B] interface GigabitEthernet 0/0/1
[USG_B-GigabitEthernet0/0/1] ip address 10.3.1.1 24
[USG_B-GigabitEthernet0/0/1] quit

[USG_B] interface GigabitEthernet 0/0/0
[USG_B-GigabitEthernet0/0/0] ip address 192.168.1.1 24
[USG_B-GigabitEthernet0/0/0] quit

[USG_B] firewall zone untrust
```

[USG_B-zone-untrust] **add interface GigabitEthernet 0/0/1**
[USG_B-zone-untrust] **quit**

[USG_B] **firewall packet-filter default permit interzone untrust trust**
[USG_B] **ip route-static 0.0.0.0 0.0.0.0 10.3.1.2**

[USG_B] **acl 3000**
[USG_B-acl-adv-3000] **rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.0 0.0.0.255**
[USG_B-acl-adv-3000] **quit**

[USG_B] **ipsec proposal tran1**
[USG_B-ipsec-proposal-tran1] **quit**
[USG_B] **ike proposal 10**
[USG_B-ike-proposal-10] **quit**

[USG_B] **ike peer a**
[USG_B-ike-peer-a] **pre-shared-key huawei**
[USG_B-ike-peer-a] **ike-proposal 10**
[USG_B-ike-peer-a] **quit**

[USG_B] **ipsec policy-template map_temp 1**
[USG_B-ipsec-policy-template-map_temp-1] **security acl 3000**
[USG_B-ipsec-policy-template-map_temp-1] **proposal tran1**
[USG_B-ipsec-policy-template-map_temp-1] **ike-peer a**
[USG_B-ipsec-policy-template-map_temp-1] **quit**

[USG_B] **ipsec policy map1 10 isakmp template map_temp**

[USG_B] **interface GigabitEthernet 0/0/1**
[USG_B-GigabitEthernet0/0/1] **ipsec policy map1**
[USG_B-GigabitEthernet0/0/1] **quit**

配置三台路由器。

Setp 11 在路由器上配置好各接口 IP 地址，并配置 OSPF 通过各接口直连网段，保证三台路由器之间路由可达即可。具体步骤省略。

[Router_A] **ospf 100**
[Router_A-ospf-100] **area 0**
[Router_A-ospf-100-area-0.0.0.0] **network 10.1.1.0 0.0.0.255**
[Router_A-ospf-100-area-0.0.0.0] **network 10.2.1.0 0.0.0.255**

```
[Router_A-ospf-100-area-0.0.0.0] quit
[Router_A-ospf-100] quit

[Router_B] ospf 100
[Router_B-ospf-100] area 0
[Router_B-ospf-100-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[Router_B-ospf-100-area-0.0.0.0] network 10.2.2.0 0.0.0.255
[Router_B-ospf-100-area-0.0.0.0] quit
[Router_B-ospf-100] quit

[Router_C] ospf 100
[Router_C-ospf-100] area 0
[Router_C-ospf-100-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[Router_C-ospf-100-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[Router_C-ospf-100-area-0.0.0.0] network 10.2.2.0 0.0.0.255
[Router_C-ospf-100-area-0.0.0.0] quit
[Router_C-ospf-100] quit
```

验证结果

1. 检查从 PC1 是否能 ping 通 PC2，如能 ping 通，在防火墙上运行 display ike sa 和 display ipsec sa 命令，查看是否已经成功建立 IPSec 隧道。
2. 查看当路由器 A 接口 down 掉时，IPSec 隧道是否还可以正常建立。

6.5 设备冗余IPSec VPN实验

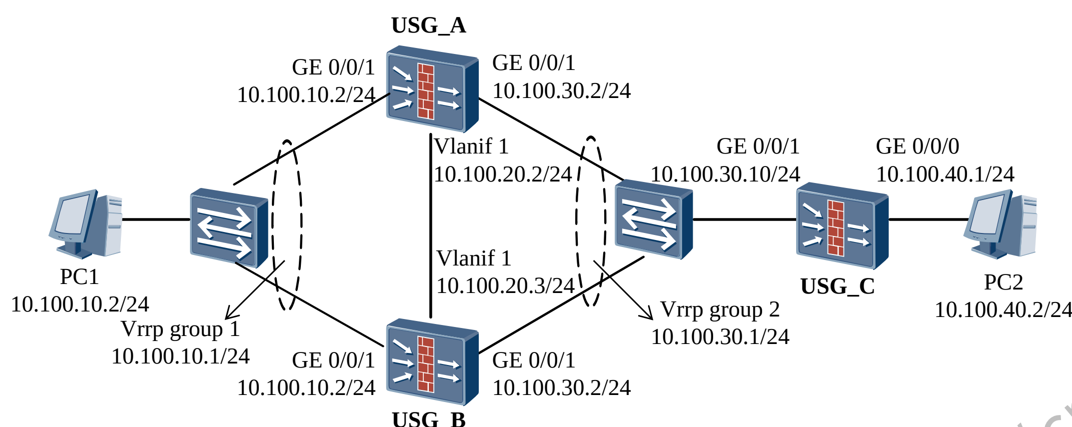
实验目的

在双机热备组网的环境下配置 IPSec VPN，使 IPSec VPN 做到设备冗余备份。

组网设备

PC 机 2 台，USG 系列防火墙 3 台，交换机 2 台。

实验拓扑图



实验步骤(命令行)

Setp 1 完成双机热备基本配置。（以主用防火墙 A 配置为例，备用防火墙 B 与防火墙 A 类似，此处省略。）

```
[USG_A]interface GigabitEthernet 0/0/0
[USG_A-GigabitEthernet0/0/0]IP address 10.100.10.2 24
[USG_A-GigabitEthernet0/0/0]vrrp vrid 1 virtual-ip 10.100.10.1 24 master
[USG_A-GigabitEthernet0/0/0]quit
[USG_A]interface GigabitEthernet 0/0/1
[USG_A-GigabitEthernet0/0/1]ip address 10.100.30.2 24
[USG_A-GigabitEthernet0/0/1]vrrp vrid 2 virtual-ip 10.100.30.1 24 master
[USG_A-GigabitEthernet0/0/1]quit
[USG_A]firewall zone trust
[USG_A-zone-trust]add interface GigabitEthernet 0/0/0
[USG_A-zone-trust]quit
[USG_A]firewall zone untrust
[USG_A-zone-untrust]add interface GigabitEthernet 0/0/1
[USG_A-zone-untrust]quit
[USG_A]firewall packet-filter default permit interzone trust untrust
[USG_A]firewall packet-filter default permit interzone local dmz
```

在本例中，使用 vlanif 接口作为心跳口。

```
[USG_A]vlan 1
[USG_A-vlan-1]port Ethernet 2/0/1
[USG_A-vlan-1]quit
[USG_A]interface Vlanif 1
[USG_A-Vlanif1]ip address 10.100.20.2 24
[USG_A]firewall zone dmz
[USG_A-zone-dmz]add interface Vlanif
```

```
[USG_A]hrp interface vlanif 1 remote 10.100.20.3
 [USG_A]hrp enable
```

Setp 2 配置防火墙 A 和防火墙 B 的 IPSec VPN 相关参数。（此处以 A 为例，防火墙 B 的配置与 A 一致。）

```
HRP_M[USG_A]acl 3001
HRP_M[USG_A-acl-adv-3001]rule permit ip source 10.100.10.0 0.0.0.255
destination 10.100.40.0 0.0.0.255
HRP_M[USG_A-acl-adv-3001]quit
HRP_M[USG_A]ip route-static 10.100.40.0 255.255.255.0 10.100.30.10

HRP_M[USG_A]ipsec proposal tran1
HRP_M[USG_A-ipsec-proposal-tran1]quit

HRP_M[USG_A]ike proposal 10
HRP_M[USG_A-ike-proposal-10]quit

HRP_M[USG_A]ike peer b
HRP_M[USG_A-ike-peer-b]ike-proposal 10
HRP_M[USG_A-ike-peer-b]remote-address 10.100.30.10
HRP_M[USG_A-ike-peer-b]pre-shared-key abcde
HRP_M[USG_A-ike-peer-b]quit

HRP_M[USG_A]ipsec policy map1 10 isakmp
HRP_M[USG_A-ipsec-policy-isakmp-map1-10]security acl 3001
HRP_M[USG_A-ipsec-policy-isakmp-map1-10]proposal tran1
HRP_M[USG_A-ipsec-policy-isakmp-map1-10]ike-peer b
HRP_M[USG_A-ipsec-policy-isakmp-map1-10]quit

HRP_M[USG_A]interface GigabitEthernet 0/0/1
HRP_M[USG_A-GigabitEthernet0/0/1]ipsec policy map1
HRP_M[USG_A-GigabitEthernet0/0/1]quit
```


📖 说明：

防火墙 B 为备用设备，IPSec 安全策略可以从主用设备备份到备用设备，但是必须手工将策略应用到接口。

```
HRP_S[USG_B]interface GigabitEthernet 0/0/1
HRP_S[USG_B-GigabitEthernet0/0/1]ipsec policy map1
HRP_S[USG_B-GigabitEthernet0/0/1]quit
```

Setp 3 在主用和备用设备上均开始 ike dpd 功能。消息发送频率 10s。确保隧道的连通。

```
HRP_M[USG_A]ike dpd on-demand 10
```

📖 说明

主设备和隧道对端设备上都需开启 IKE DPD 功能。开启后，主备设备进行切换时，隧道对端设备（USG_C）能够快速感知，并与备用设备进行隧道协商。指定 on-demand 参数，表示 DPD 工作在流量触发模式，自上次流量结束时刻算起，如果在 DPD 检测时间间隔内隧道中没有流量，则只有在有发送流量时才会发送 DPD 报文，且 DPD 检测时间从零重新计算。否则隧道中不会有 DPD 报文。

Setp 4 配置防火墙 C 的 IPSec 相关策略。

Setp 5 防火墙 C 的 IPSec 配置与 A 和 B 类似。唯一的区别在于配置防火墙 C 的 IKE peer 时，需要将对端地址指定为虚拟备份组 vrrp 2 的虚拟 IP 地址。

```
[USG_C]ike peer a
[USG_C-ike-peer-b]ike-proposal 10
[USG_C-ike-peer-b]remote-address 10.100.30.1
[USG_C-ike-peer-b]pre-shared-key abcde
[USG_C-ike-peer-b]quit
```


验证结果

从 PC1 持续 ping PC2，观察当防火墙 A 接口 down 掉时，PC1 与 PC2 的连接情况。

6.6 L2TP Over IPSec实验

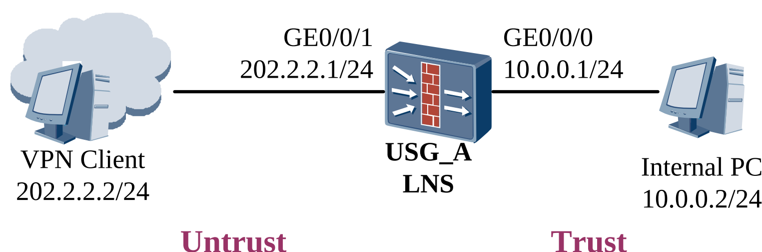
实验目的

掌握 L2TP over IPSEC 组网的配置

组网设备

PC 主机 2 台、USG 5000 系列防火墙 1 台，三层交换机 1 台

实验拓扑图



- VPN client 直接使用 secpoint 客户端建立 L2TP+IPSEC 的连接。
- USG_A 的外网 IP 地址为固定地址。

实验步骤(命令行)

Setp 1 整体网络搭建。配置各接口 IP 地址并开放域间安全转发策略，使路由可达。（具体步骤省略。）

Setp 2 防火墙 A 配置 L2TP 功能

创建对端接口分配 IP 的地址池。

```
[USG_A] aaa
[USG_A-aaa] ip pool 1 1.1.1.10 1.1.1.20
[USG_A-aaa] local-user vpdnuser password cipher Hello123
[USG_A-aaa] quit
```

创建虚拟接口模板。配置 PPP 认证方式。配置为对端接口分配 IP 地址池中的地址。

```
[USG_A] interface Virtual-Template 1
[USG_A-Virtual-Template1] ip address 1.1.1.1 24
[USG_A-Virtual-Template1] ppp authentication-mode chap
[USG_A-Virtual-Template1] remote address pool 1
[USG_A-Virtual-Template1] quit
```

配置虚拟接口模板的 IP 地址为 LNS 侧的必配项，对于 PPP 连接而言,这个地址和对端地址没有任何关系。

此处引用的地址池号要与 AAA 视图下的相对应。否则 LNS 无法为 PCB 分配地址。

配置虚拟接口模板加入安全区域。

```
[USG_A] firewall zone trust
[USG_A-zone-trust] add interface Virtual-Template 1
```

虚拟接口模板可以加入 LNS 的任一安全区域，但为 LNS 侧的必配项。

使能 L2TP 功能。

```
[USG_A] l2tp enable
```

配置 L2TP 组。

```
[USG_A] l2tp-group 1
[USG_A-l2tp1] allow l2tp virtual-template 1
[USG_A-l2tp1] tunnel authentication
[USG_A-l2tp1] tunnel password cipher Huawei123
[USG_A-l2tp1] tunnel name lns
[USG_A-l2tp1] quit
```

配置域间缺省包过滤规则。

```
[USG_A] firewall packet-filter default permit interzone local untrust
[USG_A] firewall packet-filter default permit interzone local trust
```

由于 LNS 需要给 PC 分配 IP 地址，此时不能配置确切的 ACL 及域间规则。同时，需要打开 local 和 untrust 域间的缺省过滤规则。

Setp 3 防火墙 A 上定义用于触发建立 IPSEC SA 数据流

```
[USG_A]acl 3000
[USG_A-acl-adv-3000] rule permit udp source 202.2.2.1 0 source-port eq 1701
[USG_A-acl-adv-3000]quit
```

配置域间包过滤规则

对于 untrust 与 trust 域间包过滤规则，由于使用了 L2TP over IPSEC 配置，故不存在直接的 trust 与 untrust 的直接通信,LAC 与 LNS 的域间通信的顺序为: trust-local-untrust-local-trust，故可以不配置 trust 与 untrust 之间的包过滤规则.

配置 untrust 与 local, trust 与 local 的域间包过滤规则需要使用默认放开，在 L2TP 中已配置.

Setp 4 防火墙 A 配置 IPSec 安全提议

创建名为 tran1 的 IPSec 提议。

```
[USG_A]IPSec proposal tran1
[USG_A-IPSec-proposal-tran1]transform esp
[USG_A-IPSec-proposal-tran1]encapsulation-mode tunnel
[USG_A-IPSec-proposal-tran1]esp authentication-algorithm md5
[USG_A-IPSec-proposal-tran1]esp encryption-algorithm des
[USG_A-IPSec-proposal-tran1]quit
```

Setp 5 防火墙 A 配置 IKE 提议。

```
[USG_A] ike proposal 10
[USG_A-ike-proposal-10] authentication-method pre-share
[USG_A-ike-proposal-10] authentication-algorithm sha1
[USG_A-ike-proposal-10] sa duration 86400
[USG_A-ike-proposal-10] quit
```

Setp 6 防火墙 A 配置 IKE Peer

```
[USG_A] ike peer lac
[USG_A-ike-peer-lac] ike-proposal 10
[USG_A-ike-peer-lac] pre-shared-key huawei
[USG_A-ike-peer-lac] exchange-mode aggressive
```

验证字的配置需要与对端设备相同。

Setp 7 防火墙 A 配置安全策略模板

```
[USG_A] IPSec policy-template map1tmp 10
[USG_A-IPSec-policy-templet-map1tmp-10] ike-peer lac
[USG_A-IPSec-policy-templet-map1tmp-10] proposal tran1
[USG_A-IPSec-policy-templet-map1tmp-10] security acl 3000
[USG_A-IPSec-policy-templet-map1tmp-10] quit
```

创建安全策略,引用策略模板

```
[USG_A]IPSec policy map1 10 isakmp template map1tmp
```

Setp 8 防火墙 A 引用安全策略

```
[USG_A] interface GigabitEthernet 0/0/1
[USG_A-Ethernet1/0/0] IPSec policy map1
```

Setp 9 VPN Client 配置。

新建连接向导

第一步：请选择创建方法。

HUAWEI

○ 通过导入配置文件创建连接(M)

⊙ 通过输入参数创建连接(W)

<上一步(P) 下一步(N)> 完成(F) 取消(C)

新建连接向导

第二步：请输入登录设置。

HUAWEI

LNS服务器地址(L)：200.0.0.1

登录用户名(U)：pcb

登录密码(A)：******

☐ 不保存用户名和密码(S)

<上一步(P) 下一步(N)> 完成(F) 取消(C)

新建连接向导

第三步：请输入L2TP设置。

HUAWEI

隧道名称(M)： lac

认证模式(A)： CHAP

☑ 启用隧道验证功能(E)

隧道验证密码(T)： ******

☑ 启用IPSEC安全协议(S)

◉ 预共享密钥(R)　○ 数字签名(USBKey)

身份验证字： ******

<上一步(P)　下一步(N)>　完成(F)　取消(C)

新建连接向导

第四步：请输入IPSec设置。

HUAWEI

◉ 使用LNS服务器地址(L)

○ 使用其他IPSec服务器地址(T)

<上一步(P)　下一步(N)>　完成(F)　取消(C)

新建连接向导

第五步：请输入IPSec高级设置。

HUAWEI

IPSec设置

封装模式(T)：隧道模式
安全协议(R)：ESP
AH协议验证算法(H)：MD5
ESP协议验证算法(A)：MD5
ESP协议加密算法(E)：DES
NAT穿越(S)：不启用

IKE设置

协商模式(M)：野蛮模式
ID类型(I)：IP地址
本端名字(L)：
安全网关名字(G)：
验证算法(U)：SHA-1
加密算法(O)：DES-CBC
DH组标志(D)：Group 1 (768

<上一步(P)　下一步(N)>　完成(F)　取消(C)

新建连接向导

最后一步：新建连接完成。

HUAWEI

恭喜您！VPN连接创建成功，名字为(M)：我的连接 1

<上一步(P)　下一步(N)>　完成(F)　取消(C)

实验步骤(Web)

Setp 1　配置接口 IP 地址并将各接口加入安全区域，开放域间包过滤策略。（具体步骤省略。）

Setp 2　创建 aaa 用户账号。

系统 > 管理员 > 管理员

新建管理员

用户名 vpdnuser *

密码 •••••••• *(1-16个字符)

为提升密码安全性，建议密码至少包含以下字符中的3种：<A-Z>，<a-z>，<0-9>，特殊字符（例如!，$，#，%）；且密码不能与用户或者用户的倒序相同。

确认密码 •••••••• *

用户级别 参观级

信任主机 #1

密码有效期 90 <0-999>（天）

用户有效时间设置

起始时间

结束时间

高级

应用 返回

Setp 3 启用 L2TP VPN 功能。

VPN > L2TP > L2TP

配置L2TP

L2TP 启用 应用

Setp 4 创建虚拟接口模板。

VPN > L2TP > L2TP

新建L2TP

组类型　LAC　LNS

本端隧道名称　lns

对端隧道名称　lac *

隧道密码认证

隧道密码　●●●●●●●●● *

确认隧道密码　●●●●●●●●● *

用户组　default *

新建　删除　刷新

用户名	分配固定IP

第 1 页共 1 页

用户地址分配设置

服务器地址　1 . 1 . 1 . 1 *

子网掩码　255 . 255 . 255 . 0 *

地址池起始IP　1 . 1 . 1 . 10 *

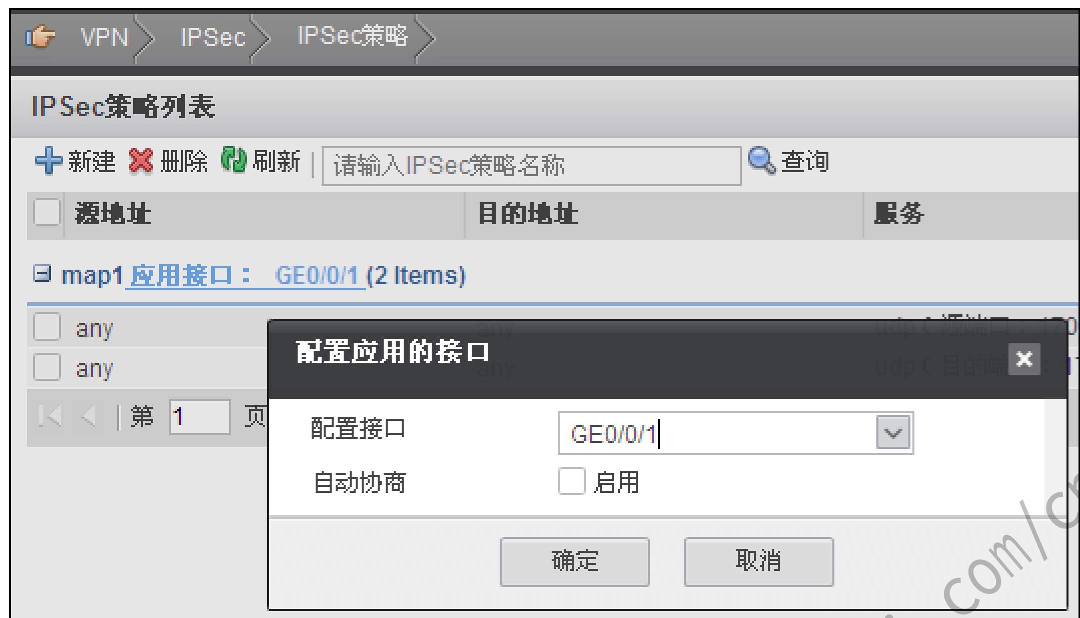
地址池结束IP　1 . 1 . 1 . 20

Setp 5　创建 IKE 协商第一阶段。

Setp 6 创建 IKE 协商第二阶段。

Setp 7 应用 IPSec 策略。选择“**VPN > IPSec > IPSec 策略**”。单击“**新建**”。在“**新建 IPSec 策略**”界面中，选择数据流配置方式为 L2TP over IPSec。单击“**应用**”。

Setp 8 将 IPSec 策略与接口绑定，选择“**VPN > IPSec > IPSec 策略**”。单击“**map1**”后的“**应用接口：- NONE -** ”。在下拉列表中选择 GE0/0/1。单击“**应用**”。



验证结果

PCB 使用 VPN Client 发起访问,之后 PCA 与 PCB 之间可以相互访问。

在防火墙上查看 IKE SA、IPSec SA 以及 L2TP 隧道建立情况。

```
[USG_A]dis ike sa
11:31:32    2013/11/20
current ike sa number: 2
-----------------------------------------------------------------------------
conn-id       peer                         flag              phase vpn
-----------------------------------------------------------------------------
40006         202.2.2.2                    RD                v1:2   public
40005         202.2.2.2                    RD                v1:1   public

  flag meaning
  RD--READY      ST--STAYALIVE    RL--REPLACED         FD--FADING
  TO--TIMEOUT    TD--DELETING     NEG--NEGOTIATING     D—DPD
[USG_A]dis ipsec sa
11:31:26    2013/11/20
===============================
Interface: GigabitEthernet0/0/1
    path MTU: 1500
===============================


  -----------------------------
  IPsec policy name: "map1"
  sequence number: 10
  mode: template
```

```
  vpn: public
  -----------------------------
    connection id: 40006
    rule number: 4294967295
    encapsulation mode: tunnel
    holding time: 0d 0h 0m 31s
    tunnel local : 202.2.2.1      tunnel remote: 202.2.2.2
    flow          source: 202.2.2.1/255.255.255.255 17/1701
    flow destination: 202.2.2.2/255.255.255.255 17/7327

    [inbound ESP SAs]
      spi: 2186095877 (0x824d2d05)
      vpn: public    said: 0    cpuid: 0x0000
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887424871/3569
      max received sequence-number: 102
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 2230748273 (0x84f68471)
      vpn: public    said: 1    cpuid: 0x0000
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887435336/3569
      max sent sequence-number: 23
      udp encapsulation used for nat traversal: N
[USG_A]dis l2tp tunnel
11:32:55  2013/11/20
 Total tunnel = 1
 LocalTID RemoteTID RemoteAddress     Port    Sessions RemoteName
 1         1          202.2.2.2         7327    1         lns
```


6.7 双机热备SSL VPN实验

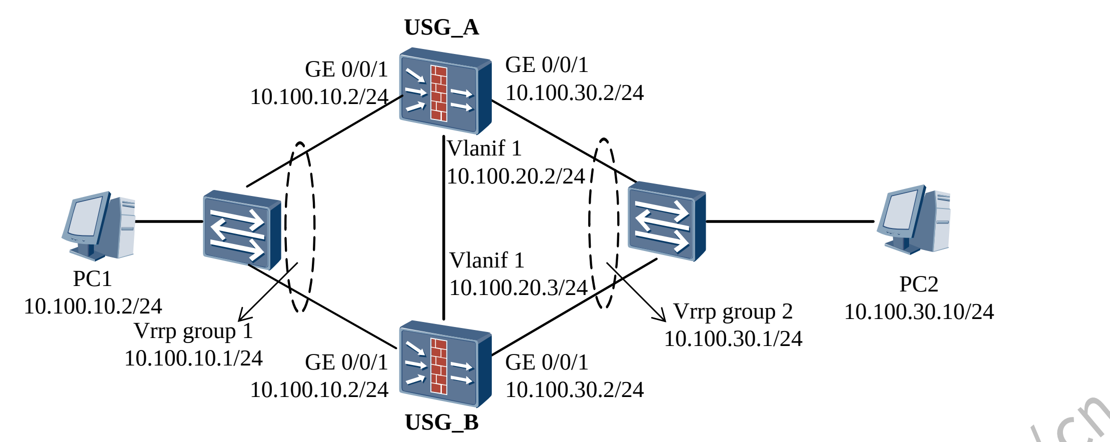
实验目的

在双机热备的组网环境下完成 SSL VPN 的功能配置。使 SSL VPN 能做到设备冗余，提高可靠性。

组网设备

PC 机 2 台，USG 系列防火墙 2 台，交换机 2 台。

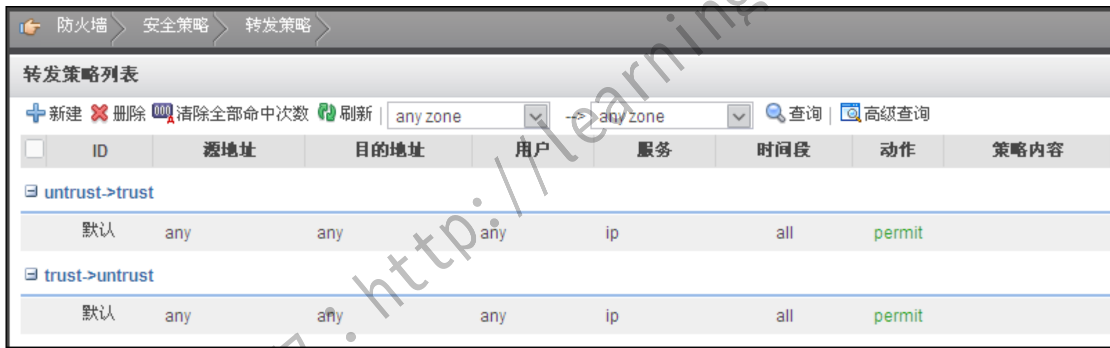
实验拓扑图



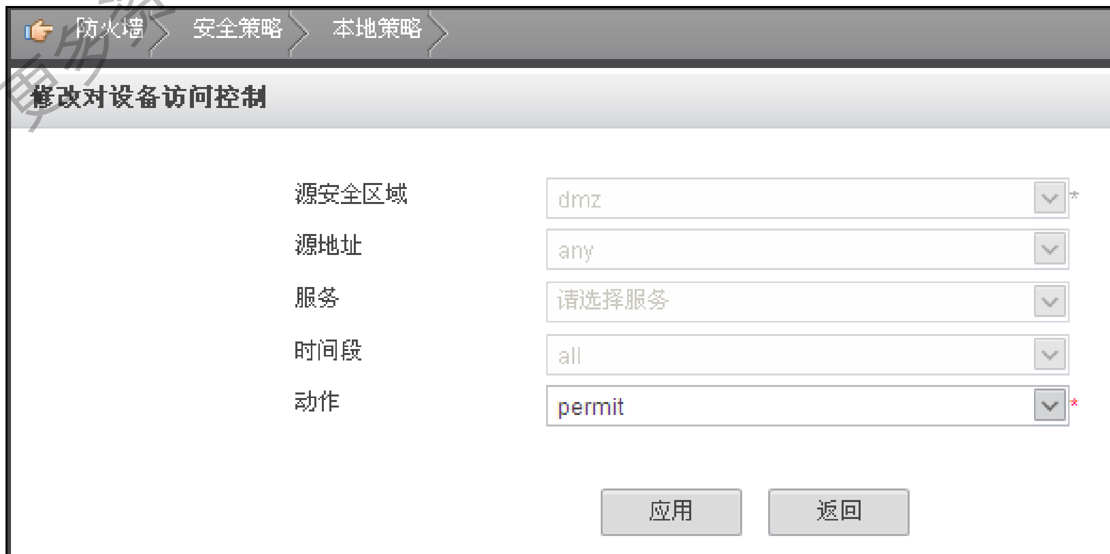
实验步骤(Web)

Setp 1　配置各接口 IP 地址并将其加入相应安全区域。（具体步骤省略）

Setp 2　配置从 trust 区域到 untrust 区域的域间安全转发策略。



Setp 3　修改本地转发策略，允许 DMZ 区域与 local 区域进行通信。使双机热备心跳口可以互联。



Setp 4 完成双机热备基本配置。（以主用防火墙 A 配置为例，备用防火墙 B 与防火墙 A 类似，此处省略。）

配置 Vrrp 备份组。

系统 > 高可靠性 > 双机热备

新建VRID

VRRP VRID 1 *<1-255>
接口名称 GE0/0/0 * 查看配置
接口IP地址/掩码 10 . 100 . 10 . 2 * 255 . 255 . 255 . 0
虚IP地址/掩码 10 . 100 . 10 . 1 * 255 . 255 . 255 . 0
管理组 Active Standby
高级
应用 返回

系统 > 高可靠性 > 双机热备

新建VRID

VRRP VRID 2 *<1-255>
接口名称 GE0/0/1 * 查看配置
接口IP地址/掩码 10 . 100 . 30 . 2 * 255 . 255 . 255 . 0
虚IP地址/掩码 10 . 100 . 30 . 1 * 255 . 255 . 255 . 0
管理组 Active Standby
高级
应用 返回

将 Ethernet 2/0/1 接口加入 VLAN 1 并配置 Vlanif 1 接口。

网络 > 接口 > 接口

新建接口

接口名称	vlanif1 *
类型	VLAN
VPN实例	public *
安全区域	dmz
VLAN ID	1 *<1-4094>
接口成员	可选：全选 FE2/0/0 FE2/0/2 FE2/0/3 FE2/0/4；已选：清空 FE2/0/1
连接类型	◉静态IP ○DHCP ○PPPoE
IP地址	10 . 100 . 20 . 2
子网掩码	255 . 255 . 255 . 0
默认网关	. . .

启用 HRP 备份功能。并将 vlanif 接口作为心跳口。

系统 > 高可靠性 > 双机热备

配置双机热备

☑ HRP启动　　HRP状态: Active　　主组状态: Active

HRP备份通道 Vlanif1 *　对端IP地址 10 . 100 . 20 . 3 *　状态： peerdown

⊞ 高级

应用　刷新

Setp 5 创建虚拟网关 SSL_VPN_VG。此处虚拟网关地址需配置为 vrrp 备份组 2 的虚拟 IP 地址。

VPN > SSL VPN > 虚拟网关管理

虚拟网关名	SSL_VPN_VG *	字母、数字或下划线，1~15个字符
虚拟网关类型	独占	
IP地址	10 . 100 . 30 . 1 *	添加IP地址
虚拟网关域名		示例: www.company.com(独占型)，vt1.company.com(共享型)，www.company.com/aa (共享型)
HTTP重定向	☐ 启用HTTP重定向服务	
最大并发用户数		1~100，默认为系统限额（系统限额：100，当前剩余可用并发用户数：100)
最大用户数	5 *	1~1000，默认为1 (系统限额：1000， 当前剩余可用用户数：1000)
最大资源数	5 *	1~1024，默认为1 (系统限额：1024， 当前剩余可用资源数：1024)

应用　返回

Setp 6 在 PC1 上创建一个 web server。配置 SSL VPN web 代理功能。

Setp 7 配置 VPNDB 用户。创建新用户（Testuser/123456）。

验证结果

在 PC2 的浏览器中输入 https://10.100.30.1 。使用配置的 VPNDB 用户名及密码登陆 SSL VPN。

观察当防火墙 A 的端口断掉连接是，PC2 对 SSL VPN 的访问是否正常。并查看防火墙双机热备切换状态。

7 防火墙攻击防范实验

7.1 搭建攻击测试环境

实验目的

安装 SEAL 攻击软件。

组网设备

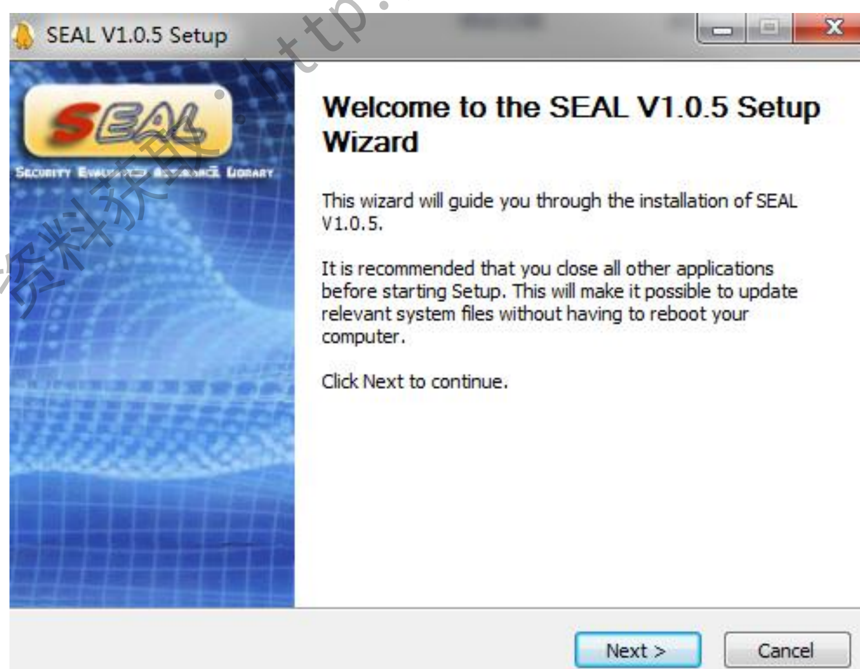
一台 Windos 32 位主机

实验拓扑图

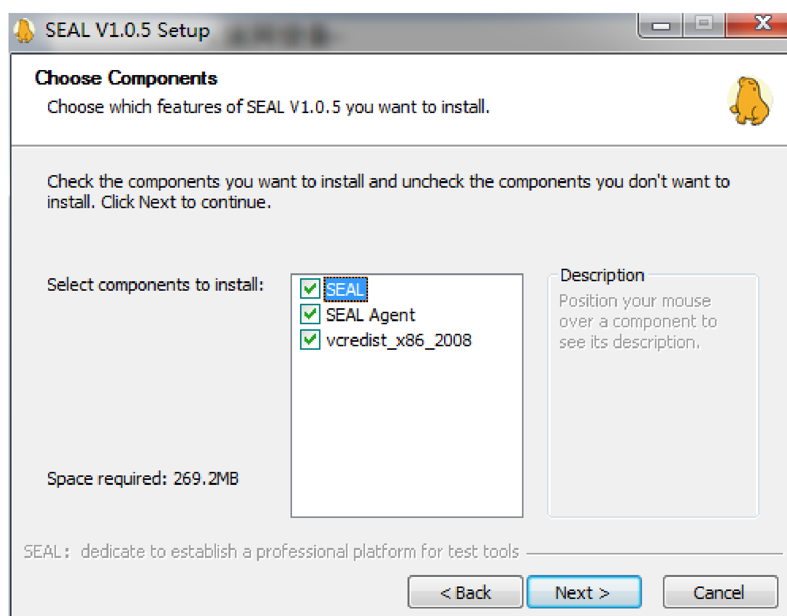
略

配置步骤

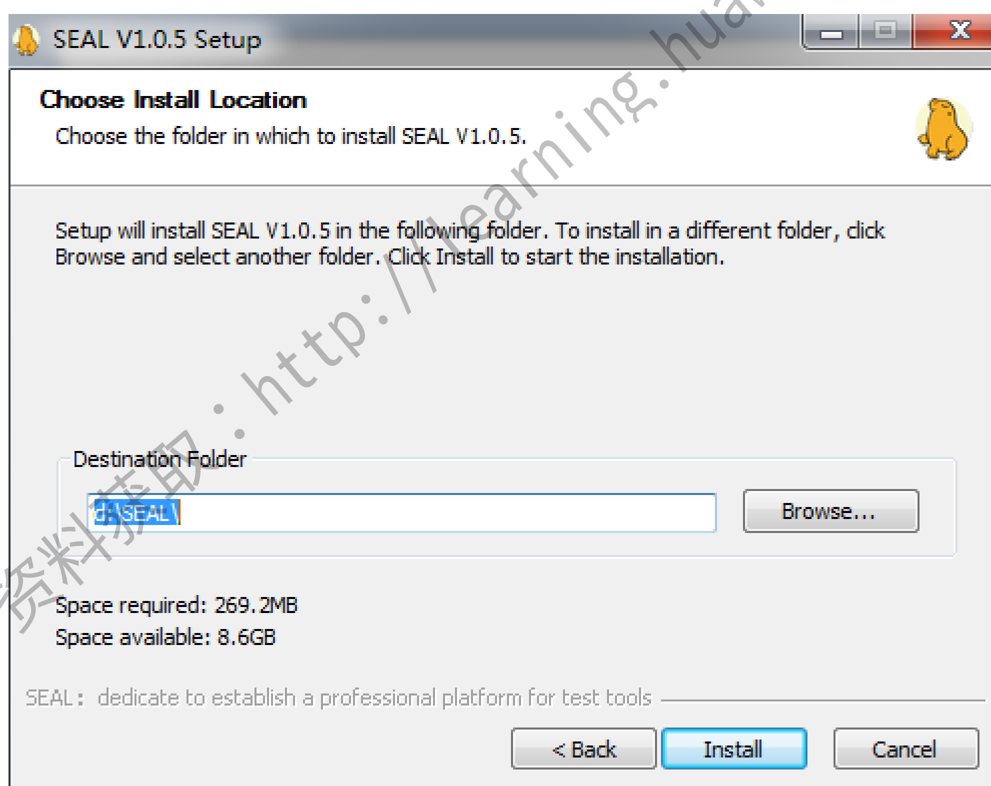
Setp 1 双击 Seal 安装文件，开始安装 Seal。



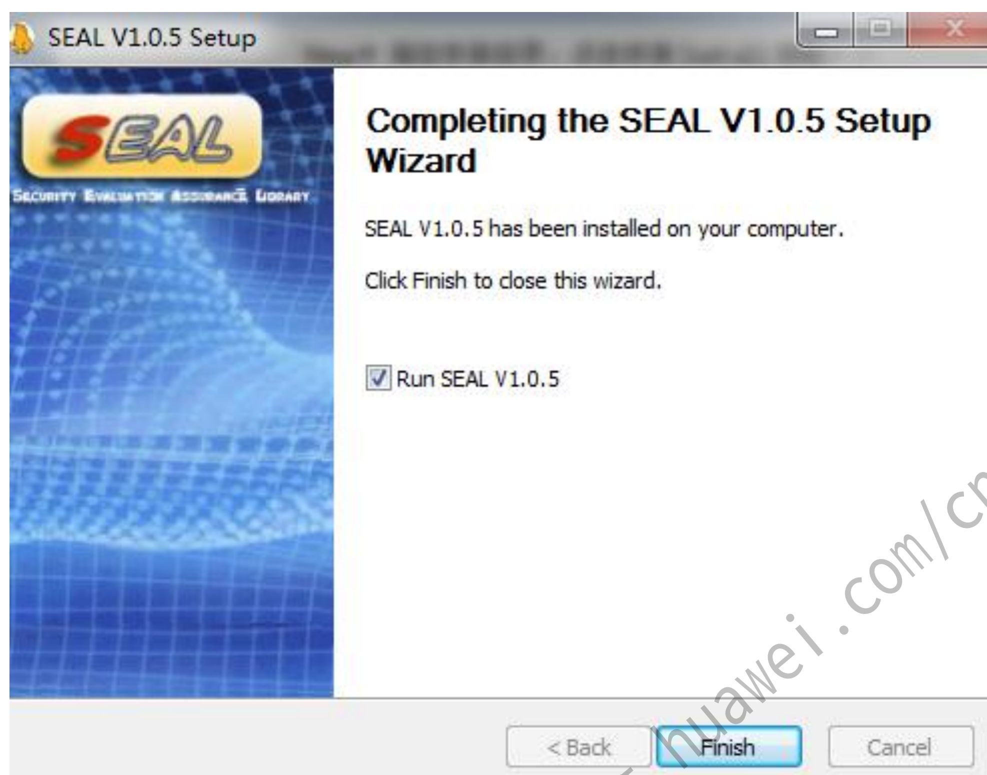
Setp 2 安装所有的 Seal 组件。



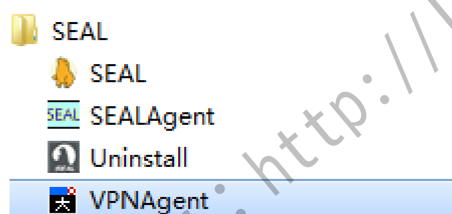
Setp 3 指定安装目录，点击安装 Install 按钮。



Setp 4 完成安装 Seal，并启动 Seal 程序。

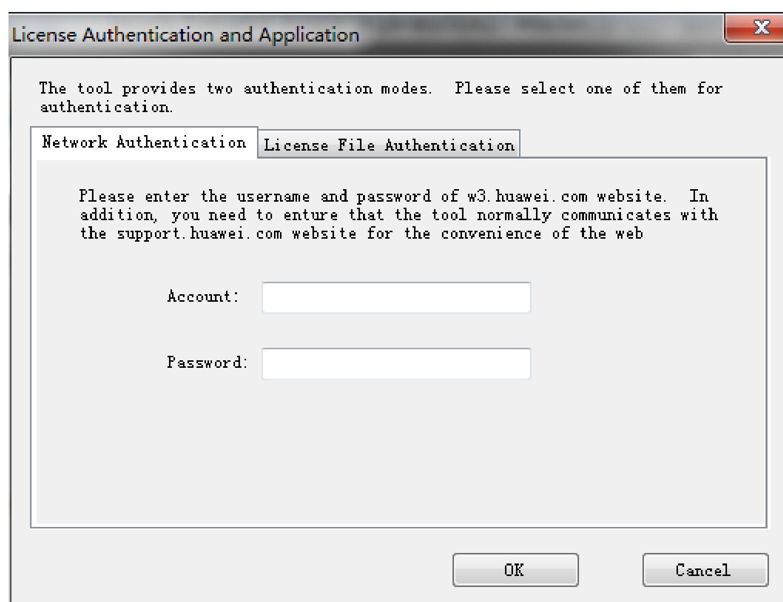


Setp 5 启动 Seal 程序，首次启动。在开始所有程序中找到 Seal 程序目录，点击 SEALAgent,启动 Agent，然后在点击 Seal，启动 Seal 程序。



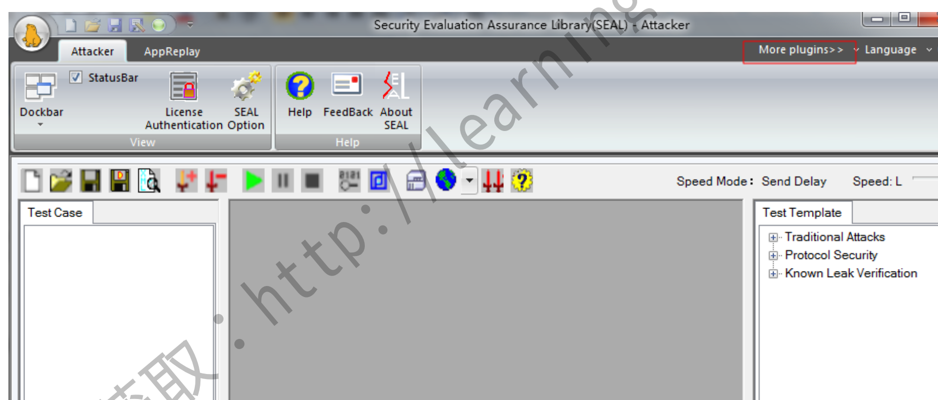
Setp 6 启动 Seal 程序后，进入 license 认证页面。Seal 需要安装 License 才可使用。有俩种方法可以激活 License:

- 输入华为员工 W3 账号和密码，并点击 OK。此时保证 PC 连接华为公司内网，方可认证成功。
- 导入 License 文件，并点击 OK。此时方式需要收集本 PC 的 ESN，并填写至指定电子流中（http://3ms.huawei.com/hi/group/6349），可自动获取 License 文件。由于电子流在研发环境，必须委托研发同事代为在电子流中申请。



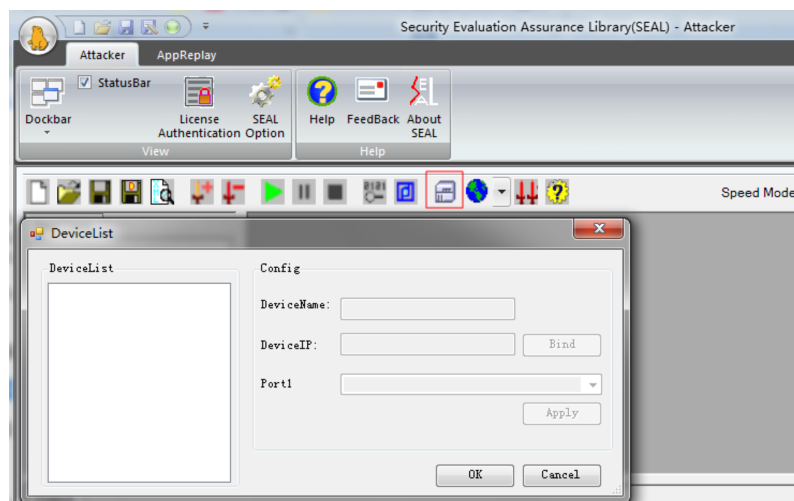
Setp 7 完成 License 的操作后，添加相应的组件。

Attacker 用于模拟 DDos 攻击。
AppReplay 用于模拟入侵攻击。



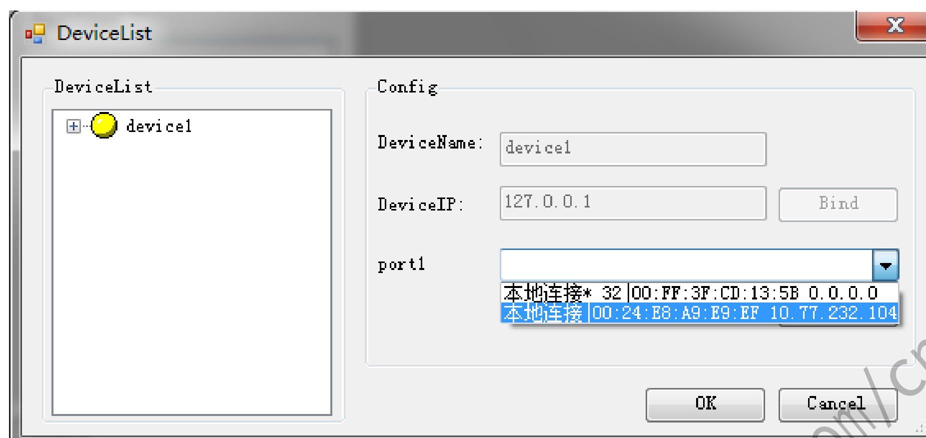
Setp 8 配置 Attacker 页面，完成初始化配置。

1) 点击设备管理，在 Devicelist 处添加 Add Device



2) 输入主机 IP 地址为 127.0.0.1（固定本机环回地址），并点击 Bind。

3) 选择使用的网卡（可以通过 IP 地址判断具体的网卡），并选择 Apply，并点击 OK。完成初始化配置。



7.2 DHCP Snooping技术

实验目的

DHCP Server 仿冒者攻击

中间人攻击与 IP/MAC Spoofing 攻击

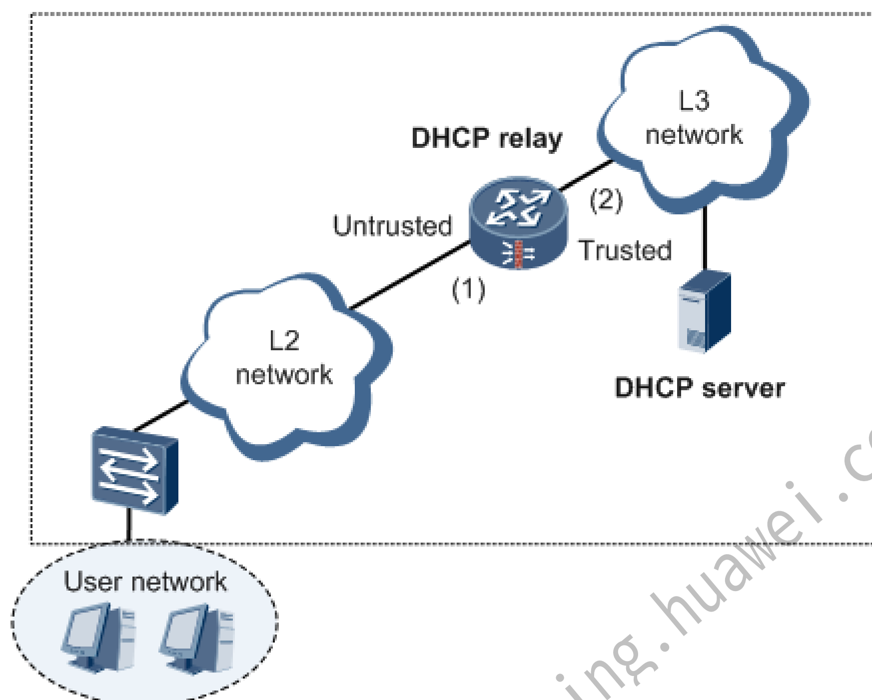
改变 CHADDR 值的 DoS 攻击

组网设备

PC1 台、DHCP Server 1 台、USG5000 防火墙 1 台

实验拓扑图

Figure 7-1 设备上应用 DHCP Snooping 典型组网图示



组网需求：

如图所示，DHCP Snooping 的作用就如同在 Client 和 DHCP Server 之间建立的一道防火墙。

DHCP Snooping 是一种 DHCP 安全特性，通过 MAC 地址限制，DHCP Snooping 安全绑定、IP + MAC 绑定、Option82 特性等功能过滤不信任的 DHCP 消息，解决了设备应用 DHCP 时遇到 DHCP DoS 攻击、DHCP Server 仿冒攻击、ARP 中间人攻击及 IP/MAC Spoofing 攻击的问题。

配置步骤

Setp 1 将接口加入安全区域，并配置域间包过滤，以保证网络基本通信正常

Setp 2 配置 DHCP Relay 基本功能

配置接口 GigabitEthernet 0/0/2 接口地址

```
<USG5000> system-view
[USG] sysname DHCP-Relay
[DHCP-Relay] interface GigabitEthernet 0/0/2
[DHCP-Relay-GigabitEthernet0/0/2] ip address 100.1.1.1 24
[DHCP-Relay-GigabitEthernet0/0/2] quit
```

#配置要实现 DHCP 中继功能接口

```
[DHCP-Relay] interface GigabitEthernet 0/0/1
[DHCP-Relay-GigabitEthernet0/0/1] ip address 10.1.1.254 24
```

```
[DHCP-Relay-GigabitEthernet0/0/1] dhcp select relay
[DHCP-Relay-GigabitEthernet0/0/1] ip relay address 100.1.1.2
[DHCP-Relay-GigabitEthernet0/0/1] quit
```

Setp 3 开启 DHCP Snooping 功能

#启用全局和接口 DHCP Snooping 功能

```
[DHCP-Relay] dhcp snooping enable
[DHCP-Relay] interface GigabitEthernet 0/0/1
[DHCP-Relay-GigabitEthernet0/0/1] dhcp snooping enable
[DHCP-Relay-GigabitEthernet0/0/1] quit
[DHCP-Relay] interface GigabitEthernet 0/0/2
[DHCP-Relay-GigabitEthernet0/0/2] dhcp snooping enable
```

Setp 4 配置 Trusted 接口

#配置 DHCP Server 侧接口为"Trusted"

```
[DHCP-Relay-GigabitEthernet0/0/2] dhcp snooping trusted
[DHCP-Relay-GigabitEthernet0/0/2] quit
```

说明：DHCP Clinet 侧所有接口开启 DHCP snooping（如果用户侧接口没有配置"Trusted"模式，那么开启了接口的 Snooping 特性后，接口模式默认为"Untrusted"），这样可以防止 DHCP Server 仿冒者攻击。

Setp 5 配置对特定报文检查和 DHCP Snooping 绑定表

#配置在 DHCP Clinet 侧接口进行 ARP 报文和 IP 报文检查

```
[DHCP-Relay] interface GigabitEthernet 0/0/1
[DHCP-Relay-GigabitEthernet0/0/1] dhcp snooping check arp enable
[DHCP-Relay-GigabitEthernet0/0/1] dhcp snooping check ip enable
```

#配置在 DHCP Clinet 侧接口进行 DHCP Request 报文检查

```
[DHCP-Relay-GigabitEthernet0/0/1] dhcp snooping check dhcp-request enable
```

#配置在 DHCP Clinet 侧接口进行 CHADDR 检查

```
[DHCP-Relay-GigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable
```

配置静态绑定表项

```
[DHCP-Relay-GigabitEthernet0/0/1] dhcp snooping bind-table static ip-address 10.1.1.1 mac-address 00e0-fc5e-008a
[DHCP-Relay-GigabitEthernet0/0/1] quit
```

Setp 6 配置 DHCP 上送速率限制

配置 DHCP 上送速率检查

```
[DHCP-Relay] dhcp snooping check dhcp-rate 90
[DHCP-Relay] dhcp snooping check dhcp-rate enable
```

Setp 7 配置 Option82

配置 DHCP 报文中携带接口信息

```
[DHCP-Relay] interface GigabitEthernet 0/0/1
[DHCP-Relay-GigabitEthernet0/0/1] dhcp option82 insert enable
[DHCP-Relay-GigabitEthernet0/0/1] quit
```

Setp 8 配置对没有表项报文的转发行为

配置对全局 ARP 报文和 IP 报文转发行为

```
[DHCP-Relay] dhcp snooping nomatch-packet arp action discard
[DHCP-Relay] dhcp snooping nomatch-packet ip action discard
```

配置对接口 ARP 报文和 IP 报文转发行为

```
[DHCP-Relay] interface GigabitEthernet 0/0/1
[DHCP-Relay-GigabitEthernet0/0/1] dhcp snooping nomatch-packet arp action discard
[DHCP-Relay-GigabitEthernet0/0/1] dhcp snooping nomatch-packet ip action discard
```

结果检查

查看全局和接口视图下 DHCP Snooping 功能状态

```
[DHCP-Relay] display dhcp snooping global
dhcp snooping enable
dhcp snooping nomatch-packet ip action discard
dhcp snooping nomatch-packet arp action discard
dhcp snooping check dhcp-rate enable
dhcp snooping check dhcp-rate alarm enable
dhcp snooping check dhcp-rate 90
dhcp snooping check dhcp-rate alarm threshold 40
```

查看 DHCP Snooping 绑定表表项信息

```
[DHCP-Relay] display dhcp snooping bind-table static
bind-table:
ifname            vrf   vsi   p/cvlan     mac-address      ip-address        tp lease
-----------------------------------------------------------------------
GE0/0/1           0000 -      0000/0000 00e0-fc5e-008a 10.1.1.1          S    0
-----------------------------------------------------------------------
binditem count:      1                        binditem total count: 1
```

显示接口上 DHCP Snooping 相关信息

```
[DHCP-Relay] display dhcp snooping interface GigabitEthernet 0/0/1
dhcp snooping enable
dhcp snooping check arp enable
dhcp snooping alarm arp enable
dhcp snooping alarm arp threshold 10
```

```
 dhcp snooping nomatch-packet arp action discard
 dhcp snooping check ip enable
 dhcp snooping nomatch-packet ip action discard
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 10
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 10
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 10
 arp total                         0
 ip total                          0
 dhcp-request total                0
 chaddr&src mac total              0
 dhcp-reply total                  0
[DHCP-Relay] display dhcp option82 interface GigabitEthernet 0/0/1
 dhcp option82 insert enable
[DHCP-Relay] display dhcp snooping interface GigabitEthernet 0/0/2
 dhcp snooping enable
 dhcp snooping trusted
 arp total                         0
 ip total                          0
 dhcp-request total                0
 chaddr&src mac total              0
 dhcp-reply total                  0
```

7.3 基于IP地址的SYN Flood攻击防范功能

实验目的

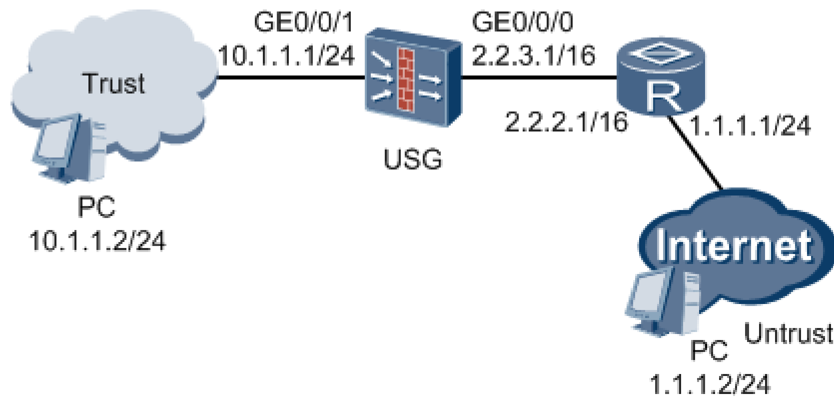
了解基于 IP 地址的 SYN Flood 攻击防范功能典型组网和配置方法。

组网设备

PC2 台、USG 5000 系列防火墙 1 台、Netfire 软件。

实验拓扑图

Figure 7-2 基于 IP 地址的 SYN Flood 攻击防范实验组网图示



USG5000 统一安全网关的以太网接口 GigabitEthernet 0/0/0 连接外部网络，以太网接口 GigabitEthernet 0/0/1 连接内部网络。需要隔离外部恶意用户对内部 IP 地址为 10.1.1.2 的 PC 的 SYN Flood 攻击行为。

配置步骤(命令行)

Setp 1 完成统一安全网关基本配置。

进入系统视图。

```
<USG5000> system-view
```

进入 GigabitEthernet 0/0/0 视图。

```
[USG5000] interface GigabitEthernet 0/0/0
```

配置 GigabitEthernet 0/0/0 的 IP 地址。

```
[USG5000-GigabitEthernet0/0/0] ip address 2.2.3.1 16
```

退回系统视图。

```
[USG5000-GigabitEthernet0/0/0] quit
```

进入 GigabitEthernet 0/0/1 视图。

```
[USG5000] interface GigabitEthernet 0/0/1
```

配置 GigabitEthernet 0/0/1 的 IP 地址。

```
[USG5000-GigabitEthernet0/0/1] ip address 10.1.1.1 24
```

退回系统视图。

```
[USG5000-GigabitEthernet0/0/1] quit
```

进入 Trust 安全区域视图。

```
[USG5000] firewall zone trust
```

配置 GigabitEthernet 0/0/1 加入 Trust 安全区域。

```
[USG5000-zone-trust] add interface GigabitEthernet 0/0/1
```

退回系统视图。

```
[USG5000-zone-trust] quit
```

进入 Untrust 安全区域视图。

```
[USG5000] firewall zone untrust
```

配置 GigabitEthernet 0/0/0 加入 Untrust 安全区域。

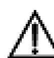
```
[USG5000-zone-untrust] add interface GigabitEthernet 0/0/0
```

退回系统视图。

```
[USG5000-zone-untrust] quit
```

配置到达 1.1.1.0 网段的下一跳路由。

```
[USG5000] ip route-static 1.1.1.0 24 2.2.2.1
```

注意：

需要配置 USG5000 到达外部特定 PC 和 Router 的静态路由。否则 USG5000 收到外部 PC 的报文后，由于无法查到路由表而丢弃该报文，导致业务不通。

 说明：

需要在 Router 上配置静态路由。此处不再赘述。

Setp 2 配置域间防火墙策略。

在 Trust 和 Untrust 域间配置防火墙策略。

```
[USG5000] policy interzone trust untrust inbound
[USG5000-policy-interzone-trust-untrust-inbound] policy 1
[USG5000-policy-interzone-trust-untrust-inbound-1] policy source 1.1.1.0 0.0.0.255
[USG5000-policy-interzone-trust-untrust-inbound-1] action permit
[USG5000-policy-interzone-trust-untrust-inbound-1] quit
[USG5000-policy-interzone-trust-untrust-inbound] quit
```

Setp 3 完成需求配置。

启用 SYN Flood 攻击防范功能。

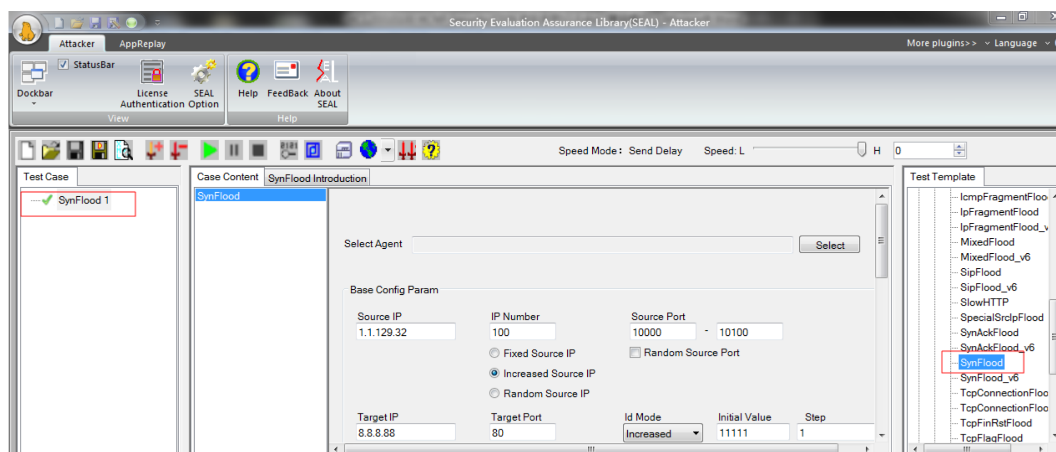
```
[USG5000] firewall defend syn-flood enable
```

配置对服务器 10.1.1.2 进行 SYN Flood 攻击防范，配置 SYN 报文的最大连接速率为 500 个/秒，启动 TCP 代理。

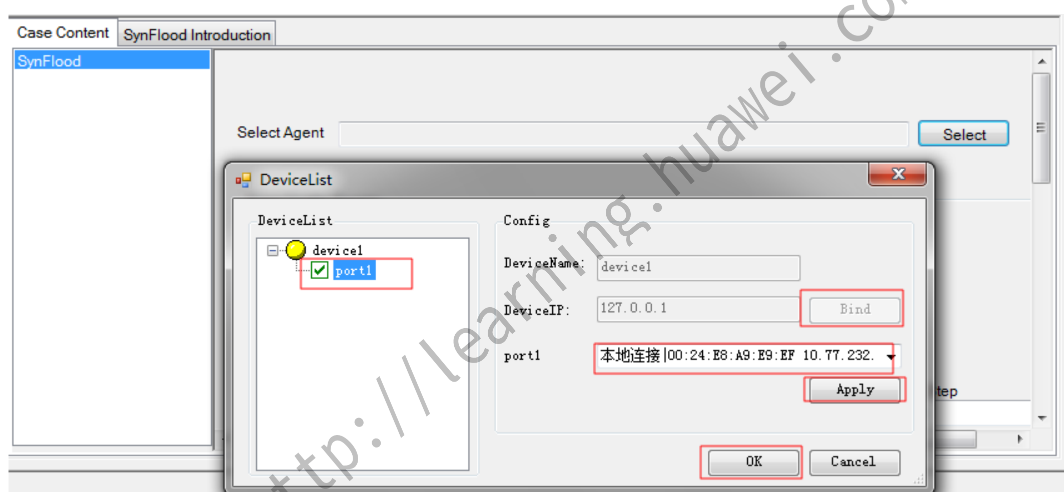
```
[USG5000]firewall defend syn-flood interface GigabitEthernet0/0/0 alert-rate 500 max-rate 500 tcp-proxy on
```

Setp 4 通过 Sear 发起攻击流量。

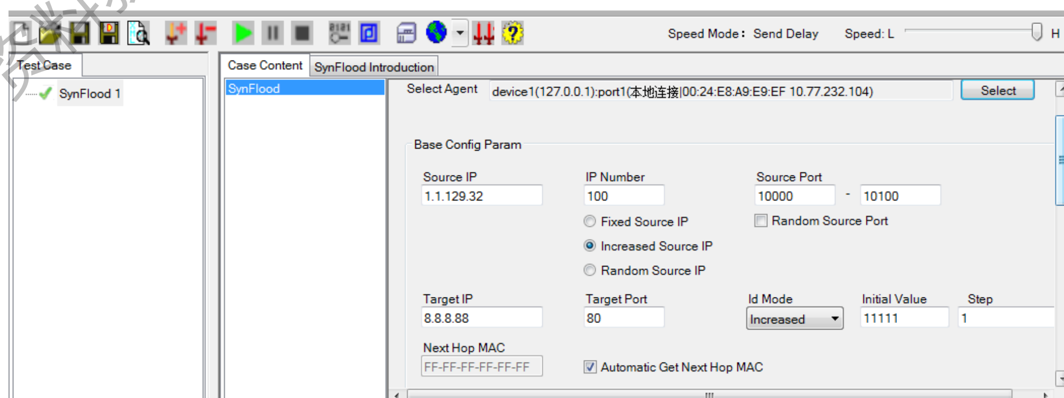
打开 Sear 测试软件的 Attacker 测试模块，在右侧的 Test Template 中，双击选择 SynFlood。这是看到左侧 Test Case 出现了 Synflood 测试项目。



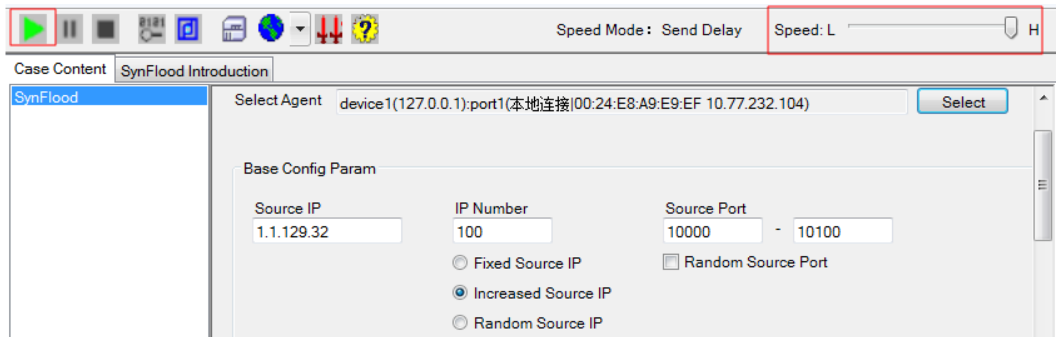
#Select Agent 绑定使用的物理网卡，依次选择 Port1，然后选择 Bind，然后选择合适的网卡，然后 Apply，最后选择 OK 按钮。



#Case Content 是测试参数，填写相应的测试参数，主要是源 IP，真实的目的 IP，其他保持默认即可。注：目的 IP 地址应该为真实的目的 IP 地址，否则将会发送全 F 的广播包。或者将 Automatic Get Next HOP MAC 取消勾选，填写任意的 Mac 地址。



#最后选择开始按钮，并通过滑动条，调整攻击报文的速度。



配置步骤(Web)

Setp 1 完成统一安全网关基本配置。 (略)

Setp 2 配置域间防火墙策略。 (略)

Setp 3 完成需求配置。

启用 SYN Flood 攻击防范功能。



配置对服务器 10.1.1.2 进行 SYN Flood 攻击防范，配置 SYN 报文的最大连接速率为 500 个/秒，启动 TCP 代理。



Setp 4 通过 Sear 发起攻击流量。 (略)

结果检查

- SYN Flood 攻防配置前，被攻击ＰＣ接受流量明显增加，ＣＰＵ占用率增加，SYN Flood 攻防配置后，被攻击ＰＣ流量及ＣＰＵ恢复正常。
- SYN Flood 攻防配置前，防火墙存在大量 TCP SYN 半连接会话，TTL5 秒，SYN Flood 攻防配置后，TCP SYN 半连接会话无法建立。

- SYN Flood 攻防配置后，防火墙打印 SYN Flood 攻击日志。
- SYN Flood 攻防配置后，查看防火墙丢包统计，存在大量 TCP SYN 报文丢弃。

7.4 TCP反向源探测方式的SYN Flood攻击防范

实验目的

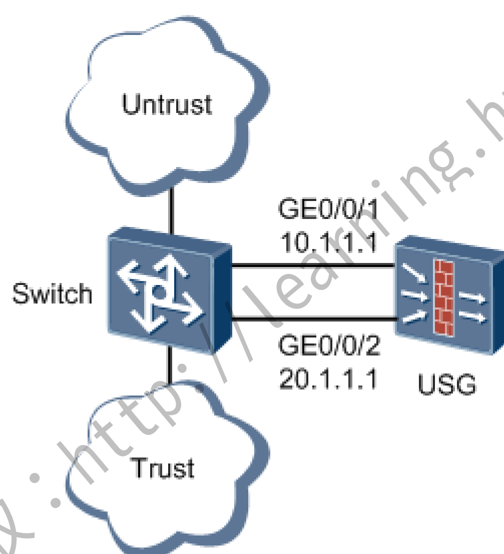
了解 TCP 反向源探测方式的 SYN Flood 攻击防范典型组网和配置方法。

组网设备

PC2 台、USG 5000 系列防火墙 1 台、Netfire 软件

实验拓扑图

Figure 7-3 TCP 反向源探测方式 SYN Flood 攻击防范实验组网图示



具体需求如下：

- USG5000 通过接口 GigabitEthernet 0/0/1 和 GigabitEthernet 0/0/2 与 Switch 连接。Untrust 区域访问 Trust 区域的报文经过 USG5000 处理后转发至 Trust 区域；Trust 区域的应答报文直接通过 Switch 发送至 Untrust 区域。
- 要求配置 TCP 反向源探测，对到达防火墙的 TCP SYN 报文进行反向探测，确定源 IP 地址为正确的 IP 地址后才允许报文通过，并配置源 IP 监控表的老化时间为 600 秒。

配置步骤(命令行)

Setp 1 完成 USG5000 的基本配置。

 说明：

此配置中只列出了与 TCP 反向源探测相关的步骤。

配置接口 GigabitEthernet 0/0/1 的 IP 地址。

```
<USG5000> system-view
[USG5000] interface GigabitEthernet 0/0/1
[USG5000-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[USG5000-GigabitEthernet0/0/1] quit
```

配置接口 GigabitEthernet 0/0/2 的 IP 地址。

```
[USG5000] interface GigabitEthernet 0/0/2
[USG5000-GigabitEthernet0/0/2] ip address 20.1.1.1 24
[USG5000-GigabitEthernet0/0/2] quit
```

将接口 GigabitEthernet 0/0/1 加入 Trust 区域。

```
[USG5000] firewall zone trust
[USG5000-zone-trust] add interface GigabitEthernet 0/0/1
[USG5000-zone-trust] quit
```

将接口 GigabitEthernet 0/0/2 加入 Untrust 区域。

```
[USG5000] firewall zone untrust
[USG5000-zone-untrust] add interface GigabitEthernet 0/0/2
[USG5000-zone-untrust] quit
```

Setp 2 配置域间防火墙策略。

在 Trust 和 Untrust 域间配置防火墙策略。

```
[USG5000] policy interzone trust untrust inbound
[USG5000-policy-interzone-trust-untrust-inbound] policy 1
[USG5000-policy-interzone-trust-untrust-inbound-1] action permit
[USG5000-policy-interzone-trust-untrust-inbound-1] quit
[USG5000-policy-interzone-trust-untrust-inbound] quit
```

Setp 3 配置 TCP 反向源探测。

在攻击报文的入接口上配置 TCP 反向源探测，最大速率为 3000 包/秒。

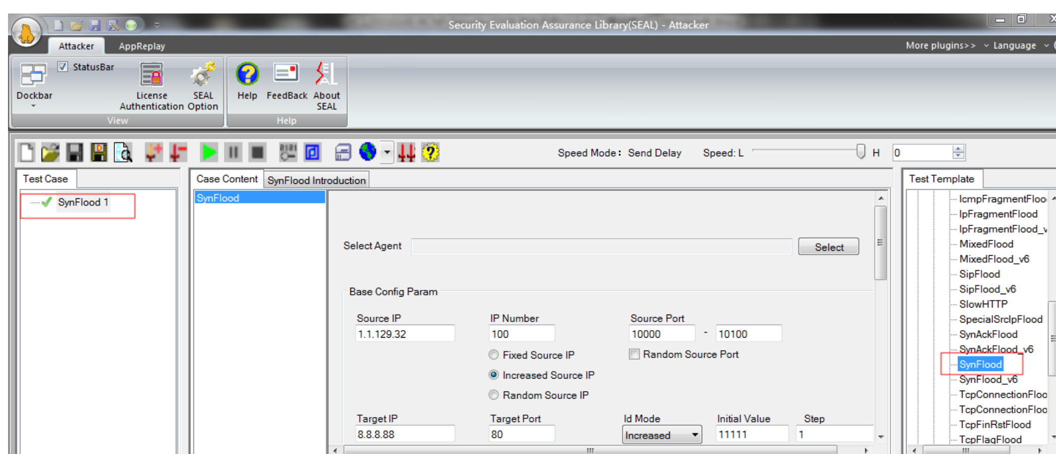
```
[USG5000] firewall source-ip detect interface GigabitEthernet 0/0/0 max-rate 3000
```

配置源 IP 监控表老化时间为 600 秒。

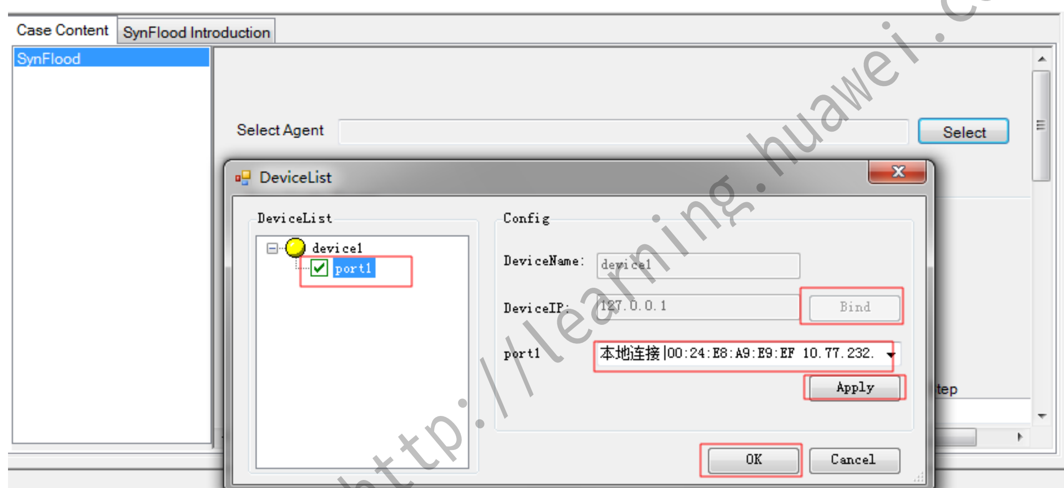
```
[USG5000] firewall source-ip detect aging-time 600
```

Setp 4 通过 Sear 发起攻击流量。

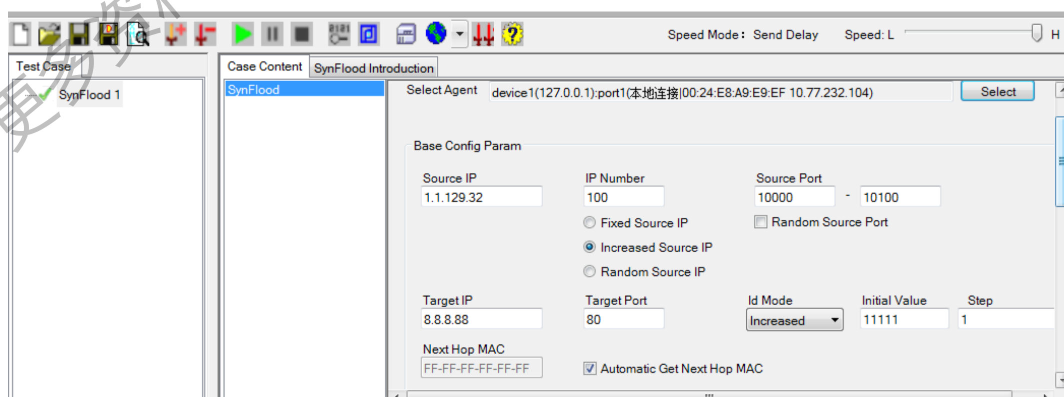
打开 Sear 测试软件的 Attacker 测试模块，在右侧的 Test Template 中，双击选择 SynFlood。这是看到左侧 Test Case 出现了 Synflood 测试项目。



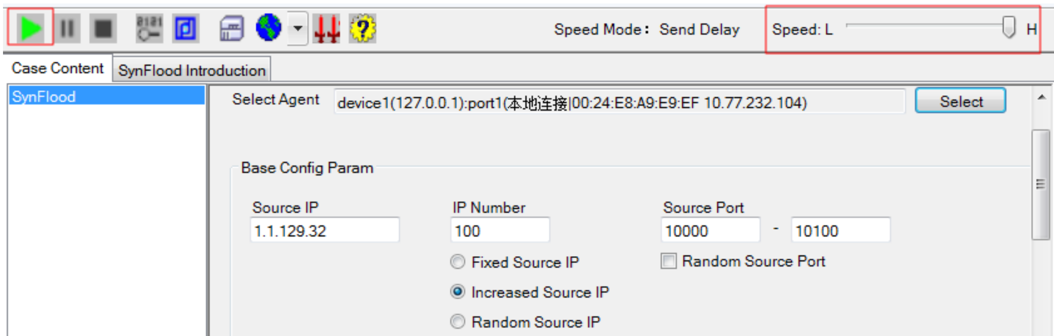
#Select Agent 绑定使用的物理网卡，依次选择 Port1，然后选择 Bind，然后选择合适的网卡，然后 Apply，最后选择 OK 按钮。



#Case Content 是测试参数，填写相应的测试参数，主要是源 IP，真实的目的 IP，其他保持默认即可。注：目的 IP 地址应该为真实的目的 IP 地址，否则将会发送全 F 的广播包。或者将 Automatic Get Next HOP MAC 取消勾选，填写任意的 Mac 地址。



#最后选择开始按钮，并通过滑动条，调整攻击报文的速度。



配置步骤(Web)

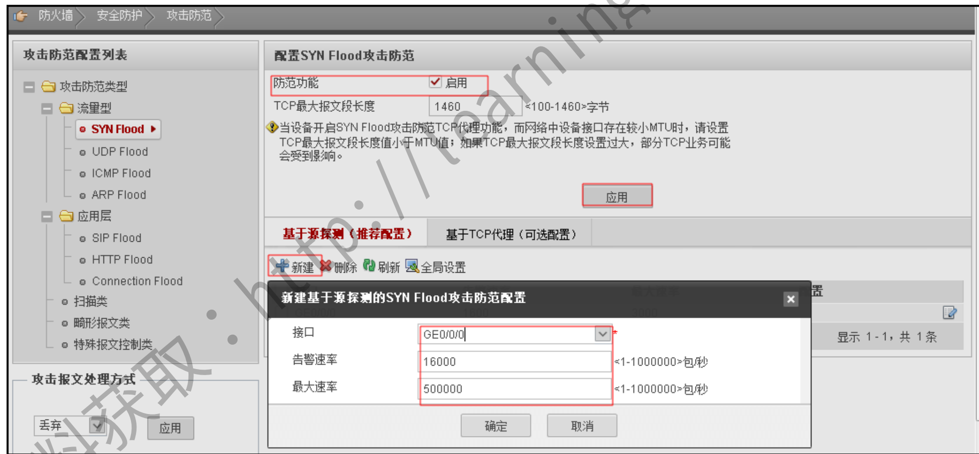
Setp 1　完成 USG5000 的基本配置。 (略)

Setp 2　配置域间防火墙策略。 (略)

Setp 3　配置 TCP 反向源探测。

在攻击报文的入接口 G0/0/0 上配置 TCP 反向源探测，告警速率为 1600 包/秒，最大速率为 3000 包/秒。

配置源 IP 监控表老化时间为 600 秒。



Setp 4　通过 Sear 发起攻击流量。

结果检查

- SYN Flood 攻防配置前，被攻击ＰＣ接受流量明显增加，ＣＰＵ占用率增加，SYN Flood 攻防配置后，被攻击ＰＣ流量及ＣＰＵ恢复正常。
- SYN Flood 攻防配置前，防火墙存在大量 TCP SYN 半连接会话，TTL5 秒，SYN Flood 攻防配置后，TCP SYN 半连接会话无法建立。
- SYN Flood 攻防配置后，防火墙打印 SYN Flood 攻击日志。
- SYN Flood 攻防配置后，查看防火墙丢包统计，存在大量 TCP SYN 报文丢弃。

7.5 基于接口的ARP Flood攻击防范

实验目的

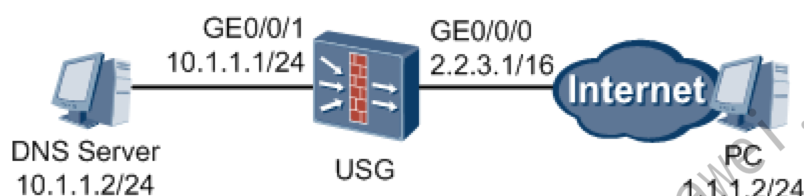
了解基于接口的 ARP Flood 攻击防范典型组网和配置方法。

组网设备

主机 2 台、USG5000 系列防火墙 1 台、Netfire 软件

实验拓扑图

Figure 7-4 基于接口的 ARP Flood 攻击防范实验组网图示



组网需求

- 统一安全网关的以太网接口 GigabitEthernet 0/0/0 连接外部网络，以太网接口 GigabitEthernet 0/0/1 连接内部网络。
- 需要隔离外部恶意用户对接口 GigabitEthernet 0/0/0 的 ARP Flood 攻击行为。

配置步骤(命令行)

Setp 1 统一安全网关基本配置。

配置 GigabitEthernet 0/0/0 的 IP 地址。

```
<USG5000> system-view
[USG5000] interface GigabitEthernet 0/0/0
[USG5000-GigabitEthernet0/0/0] ip address 2.2.3.1 16
[USG5000-GigabitEthernet0/0/0] quit
```

配置 GigabitEthernet 0/0/1 的 IP 地址。

```
[USG5000] interface GigabitEthernet 0/0/1
[USG5000-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[USG5000-GigabitEthernet0/0/1] quit
```

配置 GigabitEthernet 0/0/1 加入 Trust 区域。

```
[USG5000] firewall zone trust
[USG5000-zone-trust] add interface GigabitEthernet 0/0/1
[USG5000-zone-trust] quit
```

配置 GigabitEthernet 0/0/0 加入 Untrust 区域。

```
[USG5000] firewall zone untrust
[USG5000-zone-untrust] add interface GigabitEthernet 0/0/0
[USG5000-zone-untrust] quit
```

配置到达 1.1.1.0 网段的静态路由，此处假设下一跳为 2.2.2.1。

```
[USG5000] ip route-static 1.1.1.0 24 2.2.2.1
```

Setp 2 配置域间防火墙策略。

在 Trust 和 Untrust 域间配置防火墙策略。

```
[USG5000] policy interzone trust untrust inbound
[USG5000-policy-interzone-trust-untrust-inbound] policy 1
[USG5000-policy-interzone-trust-untrust-inbound-1] policy source 1.1.1.0 0.0.0.255
[USG5000-policy-interzone-trust-untrust-inbound-1] action permit
[USG5000-policy-interzone-trust-untrust-inbound-1] quit
[USG5000-policy-interzone-trust-untrust-inbound] quit
```

Setp 3 需求配置。

启用 ARP Flood 攻击防范。

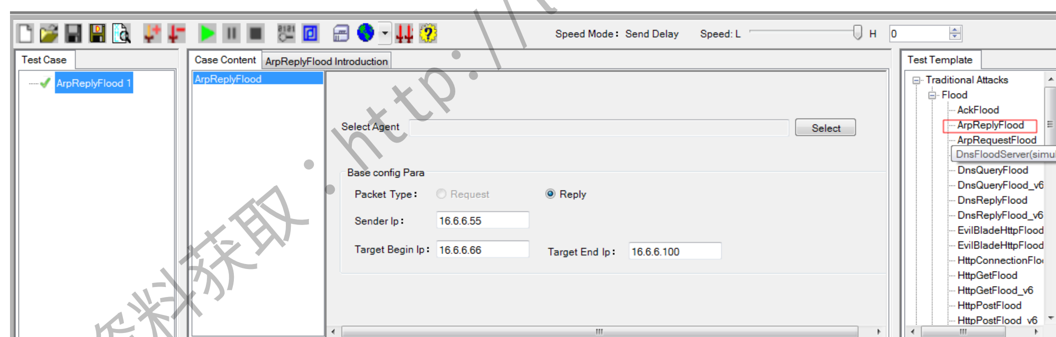
```
[USG5000] firewall defend arp-flood enable
```

打开接口 GigabitEthernet 0/0/0 的 ARP Flood 攻击防范功能开关，并配置接口的 ARP Flood 攻击防范报文速率上限阈值为 500 包/秒。

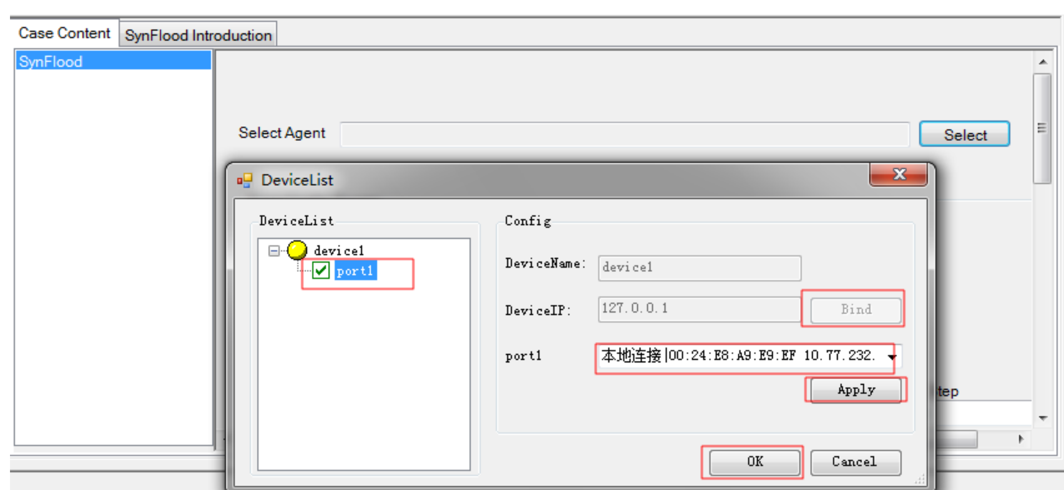
```
[USG5000] firewall defend arp-flood interface GigabitEthernet 0/0/0 max-rate 500
```

Setp 4 通过 Sear 发起攻击流量。

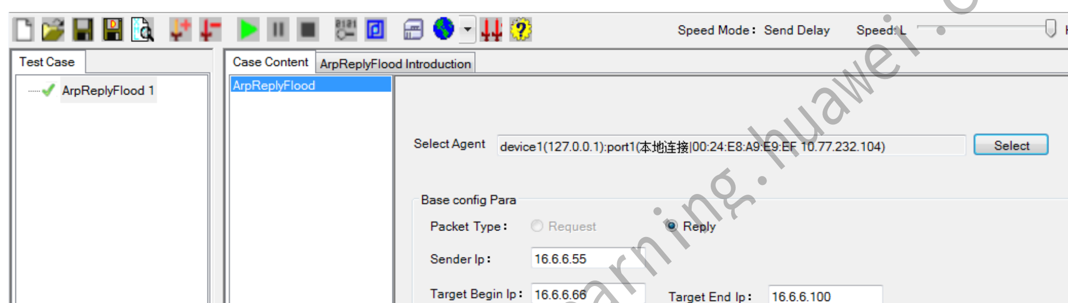
打开 Sear 测试软件的 Attacker 测试模块，在右侧的 Test Template 中，双击选择 SynFlood。这是看到左侧 Test Case 出现了 Synflood 测试项目。



#Select Agent 绑定使用的物理网卡，依次选择 Port1，然后选择 Bind，然后选择合适的网卡，然后 Apply，最后选择 OK 按钮。



#Case Content 是测试参数，填写相应的测试参数，主要是源 IP，真实的目的 IP，其他保持默认即可。



#最后选择开始按钮，并通过滑动条，调整攻击报文的速度。

配置步骤(Web)

Setp 1 统一安全网关基本配置。(略)

Setp 2 配置域间防火墙策略。(略)

Setp 3 需求配置。

启用 ARP Flood 攻击防范。

打开接口 GigabitEthernet 0/0/0 的 ARP Flood 攻击防范功能开关，并配置接口的 ARP Flood 攻击防范报文速率上限阈值为 500 包/秒。



Setp 4 通过 Sear 发起攻击流量。(略)

结果检查

- ARP Flood 攻防配置前，被攻击ＰＣ接受流量明显增加，ＣＰＵ占用率增加，ARP Flood 攻防配置后，被攻击ＰＣ流量及ＣＰＵ恢复正常。
- ARP Flood 攻防配置后，防火墙打印 ARP Flood 攻击日志。
- ARP Flood 攻防配置后，查看防火墙丢包统计，存在大量 ARP 报文丢弃。

7.6 配置地址扫描攻击防范功能

实验目的

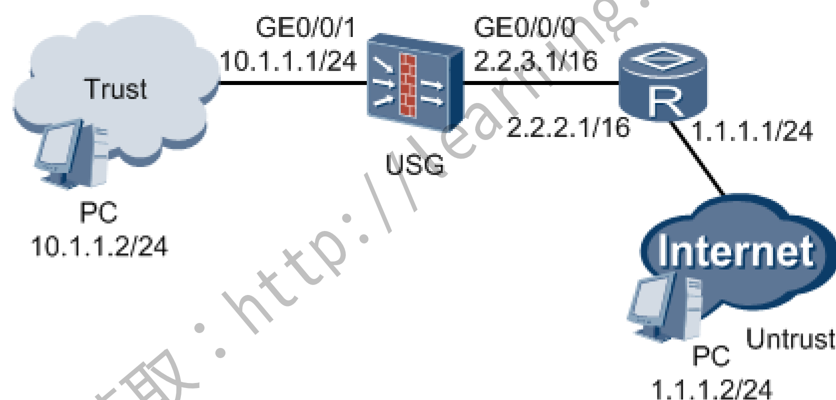
了解地址扫描攻击防范功能与配置。

组网设备

主机 2 台、USG5000 系列防火墙 1 台、Netfire 软件

实验拓扑图

Figure 7-5 地址扫描攻击防范实验组网图示



组网需求：

USG5000 的以太网接口 GigabitEthernet 0/0/1 连接 Trust 安全区域，以太网接口 GigabitEthernet 0/0/0 连接 Untrust 域。需要保护内部网络不受地址扫描的攻击。

配置步骤(命令行)

Setp 1 完成统一安全网关基本配置。

进入系统视图。

```
<USG5000> system-view
```

进入 GigabitEthernet 0/0/0 视图。

```
[USG5000] interface GigabitEthernet 0/0/0
```

配置 GigabitEthernet 0/0/0 的 IP 地址。

```
[USG5000-GigabitEthernet0/0/0] ip address 2.2.3.1 16
```

退回系统视图。

```
[USG5000-GigabitEthernet0/0/0] quit
```

进入 GigabitEthernet 0/0/1 视图。

```
[USG5000] interface GigabitEthernet 0/0/1
```

配置 GigabitEthernet 0/0/1 的 IP 地址。

```
[USG5000-GigabitEthernet0/0/1] ip address 10.1.1.1 24
```

退回系统视图。

```
[USG5000-GigabitEthernet0/0/1] quit
```

进入 Trust 安全区域视图。

```
[USG5000] firewall zone trust
```

配置 GigabitEthernet 0/0/1 加入 Trust 安全区域。

```
[USG5000-zone-trust] add interface GigabitEthernet 0/0/1
```

退回系统视图。

```
[USG5000-zone-trust] quit
```

进入 Untrust 安全区域视图。

```
[USG5000] firewall zone untrust
```

配置 GigabitEthernet 0/0/0 加入 Untrust 安全区域。

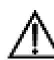
```
[USG5000-zone-untrust] add interface GigabitEthernet 0/0/0
```

退回系统视图。

```
[USG5000-zone-untrust] quit
```

配置到达 1.1.1.0 网段的下一跳路由。

```
[USG5000] ip route-static 1.1.1.0 24 2.2.2.1
```

注意：

需要配置到达外部特定 PC 和 Router 的静态路由。否则统一安全网关收到外部 PC 的报文后，由于无法查到路由表而丢弃该报文，导致业务不通。

 说明：

需要在 Router 上配置静态路由。此处不再赘述。

Setp 2 配置域间防火墙策略。

在 Trust 和 Untrust 域间配置防火墙策略。

```
[USG5000] policy interzone trust untrust inbound
[USG5000-policy-interzone-trust-untrust-inbound] policy 1
[USG5000-policy-interzone-trust-untrust-inbound-1] policy source 1.1.1.0 0.0.0.255
[USG5000-policy-interzone-trust-untrust-inbound-1] action permit
[USG5000-policy-interzone-trust-untrust-inbound-1] quit
[USG5000-policy-interzone-trust-untrust-inbound] quit
```

Setp 3 完成需求配置。

\# 启用黑名单功能。

[USG5000] **firewall blacklist enable**

\# 启用地址扫描攻击防范功能。

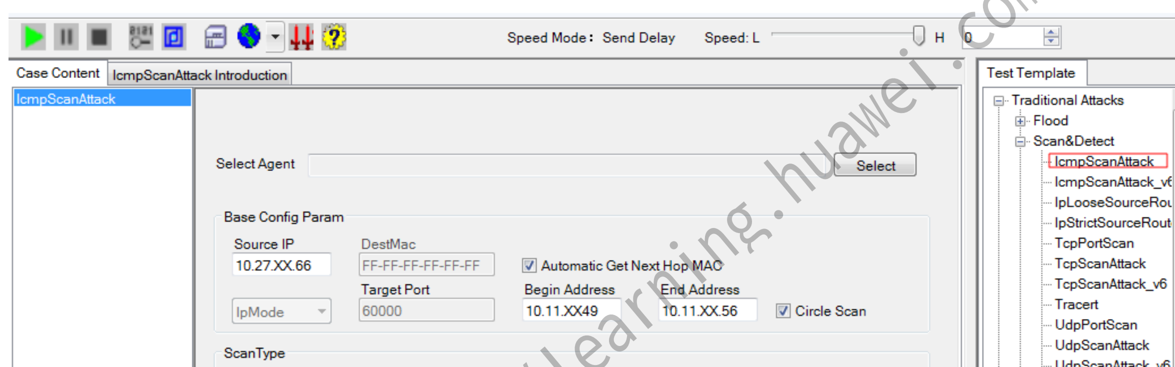
[USG5000] **firewall defend ip-sweep enable**

\# 配置地址扫描攻击防范功能。

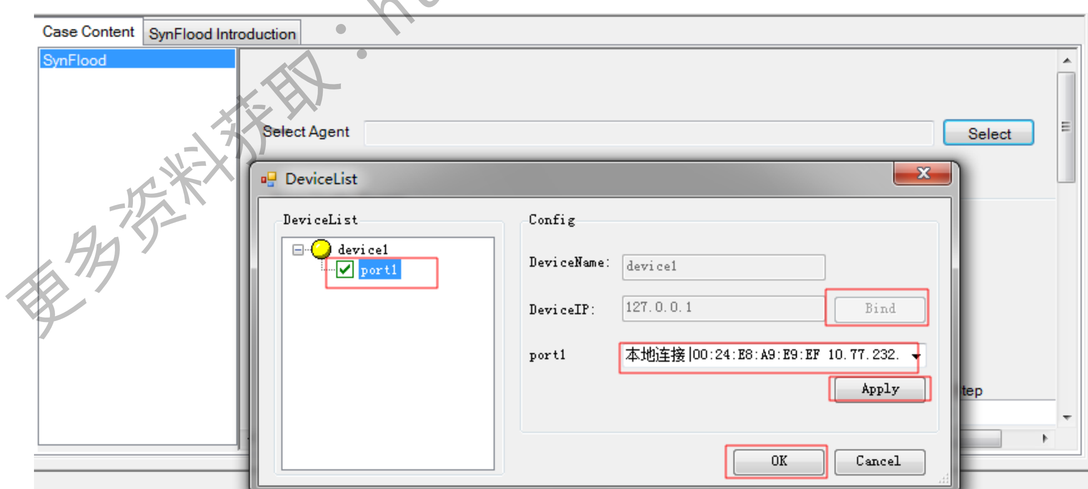
[USG5000] **firewall defend ip-sweep max-rate 1000**
[USG5000] **firewall defend ip-sweep blacklist-timeout 20**

Setp 4 通过 Sear 发起攻击流量。

\# 打开 Sear 测试软件的 Attacker 测试模块，在右侧的 Test Template 中，双击选择 ICMPscanattack。这是看到左侧 Test Case 出现了 ICMPscanattack 测试项目。



\#Select Agent 绑定使用的物理网卡，依次选择 Port1，然后选择 Bind，然后选择合适的网卡，然后 Apply，最后选择 OK 按钮。



\#Case Content 是测试参数，填写相应的测试参数，主要是源 IP，真实的目的 IP，其他保持默认即可。

\#最后选择开始按钮，并通过滑动条，调整攻击报文的速度。

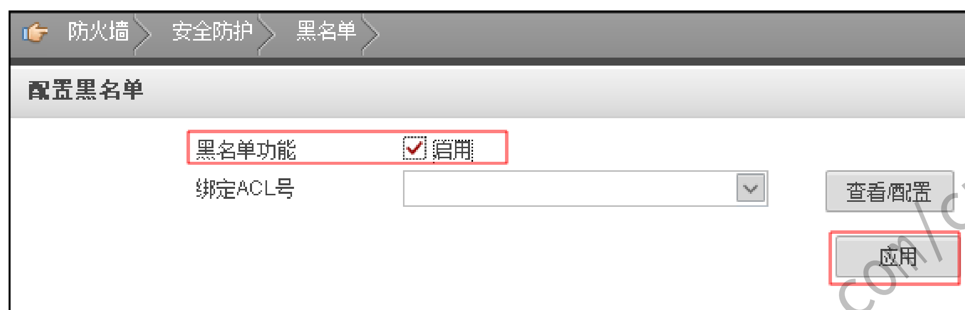
配置步骤(Web)

Setp 1 完成统一安全网关基本配置。 (略)

Setp 2 配置域间防火墙策略。 (略)

Setp 3 完成需求配置。

启用黑名单功能。



启用地址扫描攻击防范功能。

配置地址扫描攻击防范功能。



Setp 4 通过 Sear 发起攻击流量。(略)

结果检查

1. 地址扫描攻防配置前，被攻击防火墙接受流量明显增加，ＣＰＵ占用率增加，ARP Flood 攻防配置后，被攻击防火墙流量及ＣＰＵ恢复正常。
2. 扫描攻防配置后，防火墙打印 IP 扫描攻击日志。
3. 扫描攻防配置后，攻击 PC 列入黑名单，无法通过防火墙访问网络，timeout 时间过后恢复正常访问。

8 防火墙特性故障排除实验

8.1 防火墙基础特性故障排除

实验目的

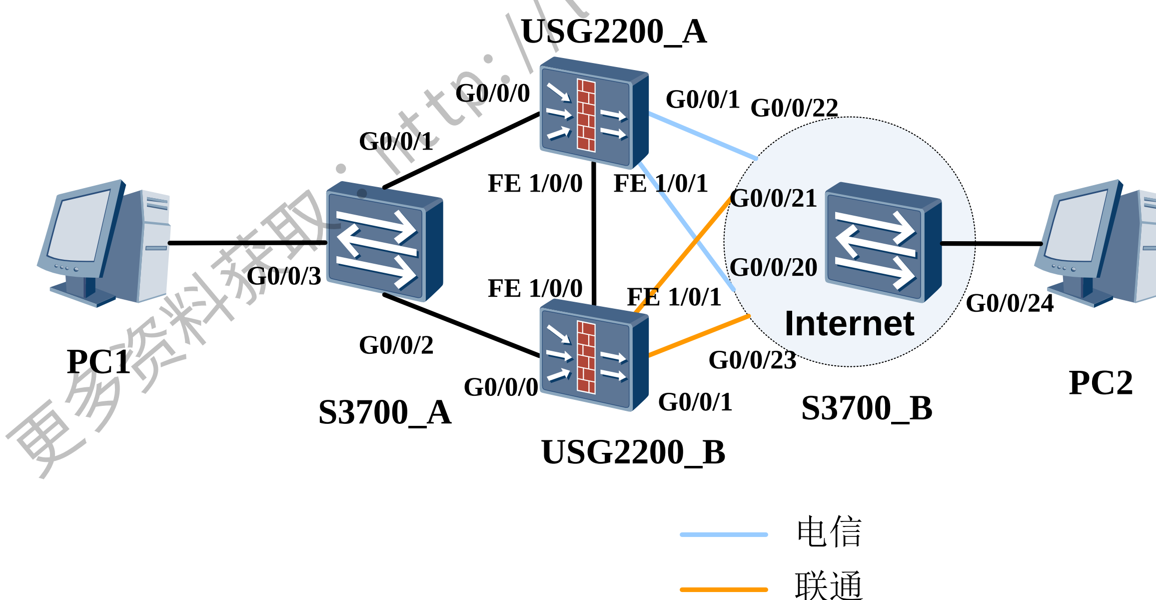
掌握防火墙 NAT 常见故障排除；

掌握防火墙双机热备常见故障排除。

组网设备

USG2130 防火墙 3 台（1 台用来模拟 internet 环境，2 台用来做双机热备）； 二层交换机 1 台； PC2 台（1 台用于模拟内网用户，1 台用于模拟 internet 用户）。

实验拓扑图



某企业为了实现 internet 的可靠接入，使用两台防火墙 USGA 和 USGB 组成双机热备接入 internet，为了增加冗余和实现流程的分担，分别租用了电信线路和联通线路。电信分配的地址段为 200.200.200.2-200.200.200.20，联通分配的地址段为 100.100.100.2-100.100.100.20 要求如下：

- USGA 和 USGB 实现双机热备，USGA 平时做为主用，当 USGA 出现故障时能切换到 USGB。
- 内网用户(PC1)通过 NAT outbound 方式上网，平时从电信链路走，当电信链路完全出现故障时，从网通线路访问 internet。
- 外网用户访问内网服务器通过联通线路走，将内网服务器通过联通地址发布。
- IP 地址规划如下：

设备	接口	IP 地址
internet(USG2130)	vlanif2(e1/0/2,e1/0/3)	200.200.200.1/24,电信
	vlanif3(e1/0/4,e1/0/5)	100.100.100.1/24，联通
	e0/0/0	201.100.100.1/24，外网用户
USGA	G0/0/0	192.168.0.2/24(virtual-ip 192.168.0.1)，内网
	G0/0/1	200.200.200.3(virtual-ip 200.200.200.2)，电信接口
	vlanif3(e1/0/1)	100.100.100.3(virtual-ip 100.100.100.2)，联通接口
	E1/0/0	10.0.0.2(virtual-ip 10.0.0.1)，热备心跳口
USGB	G0/0/0	192.168.0.3/24(virtual-ip 192.168.0.1)，内网
	vlanif3(e1/0/1)	200.200.200.4(virtual-ip 200.200.200.2)，电信接口
	G0/0/1	100.100.100.4(virtual-ip 100.100.100.2)，联通接口
	E1/0/0	10.0.0.3(virtual-ip 10.0.0.1)，热备心跳口

故障排除流程

Setp 1 故障现象描述

- USGA 和 USGB 双机热备状态不正常，未能出现 HRP_M 提示符；
- 外网无法访问 NAT Server，内网无法访问 internet；
- 内网地址为 192.168.0.251 地址转换后无法上网；
- 双机热备切换后，导致 nat 业务不通。

Setp 2 故障相关信息收集及分析

根据基本故障现象的描述，利用各种方法进一步收集相关信息，定位故障。

1、故障点：

2、信息收集方法及命令：

3、信息中的关键证据：

Setp 3 故障排除流程

请根据已知的故障现象和经验进行原因分析，并列举每一故障现象的可能原因：

1、故障现象：

2、原因列表：

3、排除过程：

讲师实验指导建议

Setp 1 分组建议

由于本实验共需 2 台 USG2230，建议 2—3 人一组，不要超过三个人。

Setp 2 组长推举以及组员分工

在分组之后，需要推举出一个组长来领导各组完成实验。组长在本组的实验过程中主要起一个牵头的作用，并组织组内的讨论。组长的推举可以采取学员毛遂自荐的方式，如果学员反应不积极，也可以有意识的指定学员中技术水平较好的来担任组长，以保证实验的顺利进行。在推举出组长之后，还可以引导组长对自己的组员也进行相应的分工。比如说可以让特定的组员负责查看配置与 display 信息；某些组员负责实际操作，修改配置；某些组员负责记录故障点和每一步操作，完成实验报告。

Setp 3 分组讨论

在实验的开始阶段，讲师应该要求各组的组长带领各组的组员先弄清网络的状况与要求，并把各设备上的配置都先读一遍，这样才不会在后面的实验中大家都弄得一头雾水。接下来可以让组长组织对故障现象，故障定位和如何解决问题进行组内的讨论。同时讲师也应该时刻关注各组的讨论情况和实验进展，并在必要的时候参与进来，把大家引导到正确的思路上来。因此，在分组讨论排除故障阶段，根据具体情况，可能会需要一到两名讲师指导实验以保证实验效果。

Setp 4 各组总结

在实验完成之后，可以请各组的组长分别对本组的实验情况作一个经验总结，包括故障的定位过程以及如何排除故障。讲师在这个时候可以鼓励各组的组员

积极的对组长的发言进行补充，讲师自己也可以针对学员的总结进行一些点评和补充。

Setp 5 提问

在各组完成总结之后，讲师可以有针对性的提一些问题，以加深学员的理解，下面列出一些问题，以供参考：

参考问题：

1．双机热备情况下，NAT 为什么要关联 vrrp id，什么情况下需要关联。

2．Nat server 域间规则设置，目标地址为什么是 inside 地址？

3．备双机热备为什么加入一个 down 的口后，主防火墙反而切换成备状态？

Setp 6 讲师总结

在本实验的最后，讲师还应该对整个实验的故障排除思路，故障点分析和解决方案做一个最终的总结，以加深学员对课程的理解，并使之更系统化。

Setp 7 实验中的时间点控制

本章节实验时间建议：

- 2 小时：讲师准备好实验环境，设置好故障点。
- 10 分钟：讲师介绍实验的网络状况和具体要求，向学员描述故障现象以及实验要求。分组并选举组长，明确各组员工的分工。
- 2 小时：各组长组织组员验证故障现象，熟悉网络状况和具体配置。对故障现象，故障定位和如何解决问题进行组内讨论，最终排除故障并完成实验报告。
- 30 分钟：各小组推举代表对故障排除结果及过程进行分享发表，讲师进行总结和点评。

8.2 VPN特性故障排除

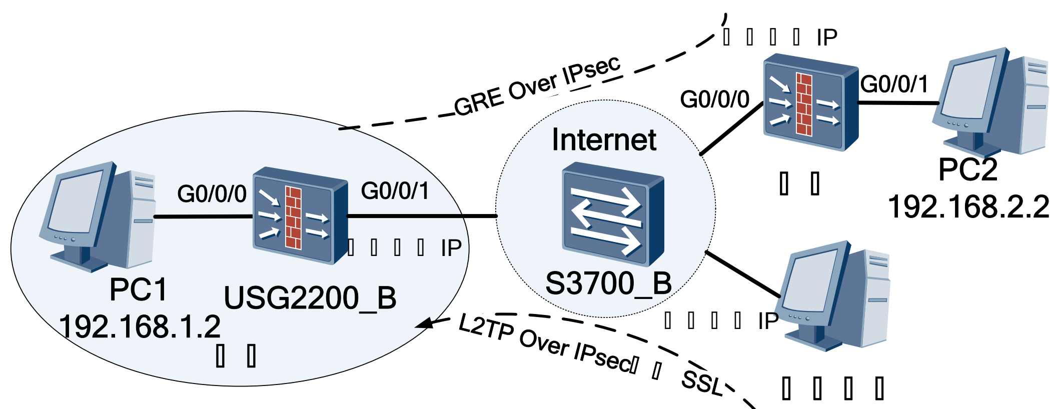
实验目的

掌握防火墙 IPSEC VPN、L2TP VPN、GRE VPN、SSL VPN 常见故障排除。

组网设备

USG2200 防火墙 2 台， 交换机 1 台（模拟 internet）；PC1 台（模拟出差用户）。

实验拓扑图



某企业有总部和分支两个办公地点，总部 A 和 B 防火墙组成 GRE OVER IPSEC VPN，出差用户使用 L2TP OVER IPSEC 或者 SSL VPN 接入 USGA，要求总部、分支以及出差用户能够互通。

故障排除流程

Setp 1 故障现象描述

GRE OVER IPSEC VPN 无法建立；

L2TP OVER IPSEC 无法建立；

SSL VPN 用户接入后，无法访问总部 192.168.1.2；

总部、分支及出差用户无法互访。

Setp 2 故障相关信息收集及分析

根据基本故障现象的描述，利用各种方法进一步收集相关信息，定位故障。

1、故障点：

____

____

____

____

____

____

2、信息收集方法及命令：

____

____

____

____

____

____

3、信息中的关键证据：

____

Setp 3 故障排除流程

请根据已知的故障现象和经验进行原因分析，并列举每一故障现象的可能原因：

1、故障现象：

2、原因列表：

3、排除过程：

讲师实验指导建议

Setp 1 分组建议

由于本实验共需 2 台 USG，建议 3 人一组。

Setp 2 组长推举以及组员分工

在分组之后，需要推举出一个组长来领导各组完成实验。组长在本组的实验过程中主要起一个牵头的作用，并组织组内的讨论。组长的推举可以采取学员毛遂自荐的方式，如果学员反应不积极，也可以有意识的指定学员中技术水平较好的来担任组长，以保证实验的顺利进行。在推举出组长之后，还可以引导组长对自己的组员也进行相应的分工。比如说可以让特定的组员负责查看配置与 display 信息；某些组员负责实际操作，修改配置；某些组员负责记录故障点和每一步操作，完成实验报告。

Setp 3 分组讨论

在实验的开始阶段，讲师应该要求各组的组长带领各组的组员先弄清网络的状况与要求，并把各设备上的配置都先读一遍，这样才不会在后面的实验中大家都弄得一头雾水。接下来可以让组长组织对故障现象，故障定位和如何解决问题进行组内的讨论。同时讲师也应该时刻关注各组的讨论情况和实验进展，并在必要的时候参与进来，把大家引导到正确的思路上来。因此，在分组讨论排除故障阶段，根据具体情况，可能会需要一到两名讲师指导实验以保证实验效果。

Setp 4 各组总结

在实验完成之后，可以请各组的组长分别对本组的实验情况作一个经验总结，包括故障的定位过程以及如何排除故障。讲师在这个时候可以鼓励各组的组员积极的对组长的发言进行补充，讲师自己也可以针对学员的总结进行一些点评和补充。

Setp 5 提问

在各组完成总结之后，讲师可以有针对性的提一些问题，以加深学员的理解，下面列出一些问题，以供参考：

参考问题：

1．GRE OVER IPSEC 和 L2TP OVER IPSEC 的 Security ACL 要如何配置，为什么要这么配置？

2．为什么要添加通过 tunnel 口的路由，缺省路由为什么不行？

Setp 6 讲师总结

在本实验的最后，讲师还应该对整个实验的故障排除思路，故障点分析和解决方案做一个最终的总结，以加深学员对课程的理解，并使之更系统化。

Setp 7 实验中的时间点控制

本章节实验时间建议：

- 2 小时：讲师准备好实验环境，设置好故障点。
- 10 分钟：讲师介绍实验的网络状况和具体要求，向学员描述故障现象以及实验要求。分组并选举组长，明确各组员工的分工。

- 2 小时：各组长组织组员验证故障现象，熟悉网络状况和具体配置。对故障现象，故障定位和如何解决问题进行组内讨论，最终排除故障并完成实验报告。
- 30 分钟：各小组选举代表对故障排除结果及过程进行分享发表，讲师进行总结和点评。

华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*）享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：*关联证书*后，请提交您的“华为账号”和注册账号的“email”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训/面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见*LVC排期*
- **4、学习工具 eNSP**
  - eNSP (Enterprise Network Simulation Platform), 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html）